MASTER EN SCIENCES INFORMATIQUES

Sécurité des données dans les systèmes d'ordinateur fonctionnant en télétraitement

Ceressia, André

Award date:
1975

Awarding institution:
Universite de Namur

Facultés Universitaires Notre-Dame de la Paix à Namur

INSTITUT D'INFORMATIQUE

Année Académique 1974-1975

Sécurité des données dans les systèmes d'ordinateur fonctionnant en télétraitement

André CERESSIA

Mémoire présenté en vue de l'obtention du grade de **Licencié et Maître en Informatique.**

"S'il a accès aux informations réservées, il ne les communiquera qu'avec parcimonie, car elles sont un des éléments importants du pouvoir."

Vance Packard

(Extrait de "La Stratégie de la Réussite")

Nous tenons à remercier particulièrement Monsieur J.-P. WINDAL, directeur du mémoire, qui nous a aidé à donner une orientation pratique et réaliste à ce travail.

Nous exprimons également notre reconnaissance envers

Messieurs G. VERBIST, A. DELAUNOY, l'équipe télétraitement d'IBM, qui ont mis leur expérience à notre disposition,

ainsi que Messieurs les Professeurs de l'Institut d'Informatique de Namur qui nous ont donné une formation de base permettant d'aborder ce travail dans d'excellentes conditions.

TABLE DES MATIERES

-o-o-o-o-o-

introduction

Depuis quelques années, il y a de plus en plus d'entreprises qui constituent leur banque de données en ordinateur et qui utilisent des terminaux pour leur mise à jour et la prise de décision.

Ces données, mémorisées sur disques et bandes, ont un caractère secret pour le monde extérieur de l'entreprise, ainsi que pour un grand nombre d'employés. Il est ainsi nécessaire d'introduire des techniques hardware et software pour conserver la confidentialité et prévoir la non-destruction de la banque de données.

Le sujet de cette étude consiste à :

- effectuer un recensement de toutes les techniques hardware et software possibles et utilisées ;
- développer un programme (software) d'identification d'utilisateur et d'autorisation d'accès à une banque de données.

Notre but est de présenter, en dehors de la portée du mémoire, une étude cohérente et suffisamment complète, à la portée de ceux qui voudrait, même en pensée, concevoir un système de sécurité des données.

CHAPITRE 1:

notions préliminaires

section 1 : bases de données et notions voisines.

I.I. NECESSITE DE METTRE EN PLACE UNE BASE DE DONNEES.

Ce serait enfoncer des portes largement ouvertes que d'insister sur les multiples inconvénients d'une informatique de gestion basée sur la création et l'exploitation de fichiers spécifiques par application ; nous citerons pour mémoire :

- saisie et stockage multiple d'une même information,
- risque de non-concordance des mises à jour,
- difficultés de rapprochement d'informations contenues dans des fichiers différents,
- tâches de maintenance des programmes rendue très pénible en cas de changement de la nature ou du format des données, etc...

Au cours des cinq à huit dernières années, un changement important est survenu dans la façon de traiter et d'exploiter les données. Le souci de supprimer ces inconvénients a engendré un concept qui en quelques années a fait fortune (dans la théorie du moins) : celui de la base de données.

Par définition, les bases de données reposent sur la notion d'intégration par opposition à une organisation par applications cloisonnées, articulées autour d'une multitude de fichiers de formes et de structures différentes, contenant de nombreuses informations redondantes, et traitées par des programmes de création, de mise à jour et de consultation différents.

Le terme base de données désigne une collection centralisée de toutes les données stockées pour les besoins d'une ou de plusieurs applications interdépendantes.

La mise en place d'une base de données suppose le développement ou l'acquisition d'un software particulier permettant de la gérer ; ce software (SGBD ou système de gestion de bases de données) doit assurer l'interface entre les programmes d'application et la base de données.

Les objectifs du SGBD tels qu'ils ont été définis par le Dâta Base Task Group du CODASYL peuvent être résumés de la façon suivante :

- permettre la structuration des données de la manière la plus adaptée à chaque application sans égard au fait que tout ou partie de ces données peuvent être utilisées par d'autres applications, ceci, tout en évitant la redondance des données ;
- Permettre à plusieurs applications de se servir concurremment d'une même base de données ;
- fournir et permettre l'utilisation de plusieurs stratégies de recherche de données dans la base entière ou dans une partie de cette base ;
- protéger la base de données contre des accès non-autorisés ;
- centraliser la localisation physique des données ;
- rendre les programmes indépendants de l'affectation physique des fichiers ;
- permettre la spécification de structures de données variées allant de constituants sans relation entre eux jusqu'à des réseaux ;
- permettre à l'utilisateur de se servir des données sans avoir à se préoccuper de la réalisation des relations qui ont été déclarées entre constituants ;
- rendre les programmes aussi indépendants des données que la technique actuelle le permet ;
- séparer la description de toutes les données de la base et les données effectivement accessibles à un utilisateur ;
- fournir une description de la base qui puisse être utilisée par plus d'un langage de traitement ;
- avoir une architecture permettant un interface entre la base de données et plusieurs langages.

En résumé, le SGBD prend en charge la création, la structuration, l'organisation, la mise à jour et la maintenance de la base de données, y compris les mesures de sauvegarde et de sécurité.

Exemples de SGBD :

a) chez les grands constructeurs :

- SOCRATE (CII); IDS (HONEYWELL-BULL),
- IMS (IBM), DMS2 (ICL), DMS 1100 (UNIVAC),
- FORTE (BURROUGHS), TOTAL (CINCOM SYST. INT.),
- ABADAS (TELSYS), IDMS (METRA INTERN.), GIM (MATRA),
- PHOLAS (PHILIPS) (UNIDATA), SESAM (SIEMENS)

b) chez les petits constructeurs :

- DMS (LOGABAX), FAMOUS (NCR)

I.2. LA BASE DE DONNEES : UN PREMIER PAS VERS UN SYSTEME INTEGRE DE GESTION (MIS ou Management Integrated/Information System)

Ces dernières années, l'ordinateur a acquis une fonction prépondérante d'instrument de direction ; les entreprises et l'administration font de plus en plus appel aux installations de traitement électronique de l'information comme outils dans la prise de décisions.

Les charges imposées de nos jours par la complexité de la direction de l'entreprise imposent à celle-ci la mise en place d'un système intégré de gestion c'est-à-dire d'un programme (ou d'une collection de programmes) d'application qui, à partir des données extraites par le système de gestion de la base, fournit des informations sous une forme directement exploitable par l'utilisateur.

Outre son aide à la prise de décisions, il est l'outil de gestion complète de l'entreprise.

Exemple : dans une entreprise métallurgique, le système d'ordinateur peut reprendre :

- l'enregistrement des commandes ;
- le planning et le contrôle de production de chaque engin de production ;
- la facturation, la gestion du stock de pièces de rechange etc...

Un arrêt prolongé du système d'ordinateur risque de provoquer certains problèmes de production dans l'usine.

I.3. BASES DE DONNEES ET TELETRAITEMENT.

Tous les utilisateurs exigent actuellement un accès direct et rapide à des informations explicites et à jour. Le nombre croissant de banques de données et leur développement ainsi que celui des systèmes de télétraitement mettent en évidence cette tendance. L'introduction de solutions avancées et intégrées a été en grande partie facilitée par l'emploi de langages de programmation évolués et par la mise en service de banques de données et de systèmes de transmission de données.

Les SGBD les plus sophistiqués actuellement disponibles sur le marché offrent des possibilités d'accès à la base de données en télétraitement. Remarquons que les deux notions sont cependant bien distinctes : le télétraitement peut exister en l'absence de base de données, de même que celle-ci peut parfaitement vivre et prospérer sans télétraitement si le besoin ne s'en fait pas sentir.

I.3.I. DEFINITION.

Par télétraitement, on désigne tout un ensemble de techniques qui consistent à exploiter des ressources ordinateur à distance.

I.3.2. MODES D'EXPLOITATION RELEVANT DU TELETRAITEMENT :

On distingue :

- le remote batch (ou traitement par lot à distance), qui consiste à envoyer des trains de travaux à partir d'un terminal pour être traités et restitués après traitement;

- le time-sharing dont le principe repose sur une répartition de ressources machines entre plusieurs utilisateurs travaillant en même temps ;
- le temps réel appliqué à des problèmes de processus industriel et de gestion de transactions :

  . applications industrielles : télécommande et télémesure.

  - l'ordinateur est lié à des instruments de mesure.
  - Il doit réagir à des événements dont l'existence est limitée.
  - le temps de réponse est strictement borné et s'exprime en dixièmes ou millièmes de seconde.
  - l'ordinateur est en fait un miniordinateur.
  - la durée de vie escomptée de l'application varie entre 5 et 30 ans.

  . applications de gestion : gestion de transactions.

  - Dialogue entre hommes et ordinateur, à partir de terminaux conversationnels.
  - Accès direct; instants aléatoires d'appel à l'ordinateur ; concurrence éventuelle.
  - Temps de réponse limité par la patience des opérateurs; en pratique : de l'ordre de la seconde.
  - Mini ou gros ordinateur.
  - La durée de vie escomptée des systèmes en temps réel varie de 5 à 8 ans.

  Exemple : tenue à jour de fichiers en temps réel (+ traitements annexes en temps différé)

  - Saisie des données TR : 0,2 s.
  - Interrogations TR : 5,0 s.
  - Transactions TR : 10,0 s.

I.3.3. REMARQUES.

Le temps de réponse étant évidemment variable suivant les informations traitées et les objectifs de l'application, nous n'insisterons pas davantage sur la nécessité de considérer ici un système temps réel avec ses différents aspects (multitasking, synchronisation des tâches, traitements périodiques, gestion des interruptions, allocation des ressources, etc...)

Dans ce mémoire, seul l'aspect télétraitement sera retenu. Le système répondra dans un délai qui correspond à l'échelle de temps auquel se déroulent les événements dans le système considéré. En fait, toute l'échelle se rencontre de la milliseconde (contrôle de processus) à l'heure.

section 2 : nécessité d'envisager un système de sécurité.

2.I. DESCRIPTION DU SYSTEME DE TELETRAITEMENT RETENU DANS LE CADRE DE CE MEMOIRE.

D'un point de vue software, le télétraitement est géré par un sous-ensemble du système d'exploitation qui doit réaliser trois fonctions principales :

- la fonction de contrôle du réseau ;
- la gestion des messages ;
- la gestion des programmes d'application.

L'ensemble des usagers est géré par un seul JOB, mais à l'aide d'un moniteur de télétraitement.

Le moniteur assure :

1) la gestion des messages : elle consiste à

- gérer les files d'attente d'entrée ou de sortie en fonction de certaines classes de priorité ;
- recomposer les messages ;
- générer des procédures particulières en cas d'erreur ;
- établir certaines statistiques ;
- tenir les comptes et un journal de transactions ;
- lancer le traitement qui leur convient ; (A chaque type de message correspond en effet un programme qu'il convient d'appeler en mémoire s'il n'est pas résidant.)

Remarque : Les files d'attente de messages seront implantées soit :

. en mémoire centrale,
. en mémoire secondaire,

ou gérées par un ordinateur frontal qui déchargera ainsi totalement le calculateur des procédures d'entrée-sortie.

2) La gestion des lignes et des terminaux:

- indique au terminal quand il doit émettre ;
- assure la synchronisation des messages avec celui-ci ;
- réalise la gestion des tampons d'entrée-sortie en affectant une zone à chaque terminal.

3) La gestion de la mémoire :

- réalisée suivant le principe de l'allocation dynamique des ressources mémoire :

  Cette technique consiste à diviser la mémoire en pages I K environ, qui sont affectées par le superviseur soit à des données (en provenance de la base), soit à des programmes (stockés sur mémoires auxiliaires) pendant le déroulement de la transaction.

4) La gestion des files d'attente :

Il existe plusieurs types de files d'attente situées à différents niveaux du déroulement de la transaction.

a) niveaux : - files des messages en entrée et sortie ;
- files d'attente des canaux ;
- files d'attente des travaux en cours de traitement.

b) types de files d'attente :

- files d'attente séquentielles (FIFØ)
  ex. : cas des messages arrivant au calculateur ;
- files du type LIFO
  ex. : file servant à la gestion des pages libres en mémoire (où l'affectation d'une page est effective dès qu'elle est libre ;
- files d'attente non ordonnées
  ex. : extraction des messages traités par le même programme d'application en vue d'une optimisation des accès disque ;
- files d'attente à priorités multiples
  ex. : lorsque des messages ou des terminaux ont une plus grande priorité que d'autres. (Le Sceduleur fera passer des messages d'une file vers une autre.)

Remarque : Lors de la conception du système, on doit prévoir et calculer la longueur de la file d'attente et veiller à ce qu'elle ne devienne pas infinie. (Simulation ou de façon analytique par la théorie d'Erlang.)

2.2. RESUME.

Les programmes d'application sont gérés par un superviseur autonome, le moniteur, qui est résidant dans une partition mémoire. C'est le moniteur qui, en fonction des messages à traiter, active l'un ou l'autre des programmes qui sont soit stockés sur disques, soit directement résidants dans la partition.
L'utilisateur communique avec son programme par l'intermédiaire de transactions ; chacune d'elle renferme un code ; chaque code correspond à un ou plusieurs programmes.
C'est le programme d'application qui réalise donc le déroulement proprement dit de la transaction. Il communique avec les terminaux, les fichiers et réalise le traitement qui correspond au type de la transaction.

2.3. ELEMENTS JUSTIFIANT L'INSTAURATION DE MESURES DE SECURITE.

La nécessité de mettre en place des mesures de sécurité résulte de deux situations de fait :

Primo : - ce que l'on pourrait appeler le progrès dans le domaine de l'informatique : développement des bases de données, possibilités de gestion intégrée de l'entreprise, progrès hardware. (voir section I)

Secundo:- ce que l'on pourrait définir comme les "expériences néfastes"; ici, nous touchons la rubrique des faits divers de la presse écrite.

- exemples : . espionnage industriel :

Comme l'ordinateur peut être l'outil de recherche, de production et de gestion d'une société, des données confidentielles peuvent sortir de l'entrepris (bandes magnétiques, documents d'imprimantes...)

. fraudes internes :

Si la gestion financière d'une entreprise est confiée à un ordinateur, un membre du personnel peut trafiquer le programme ou les programmes de gestion financière à son profit personnel.

. destructions :

Comme l'ordinateur devient un outil de fonctionnement d'une entreprise, la destruction (incendie, inondations, sabotage, ...) du système (hardware ou software) peut poser pas mal de problèmes.

2.3.I. DANGERS PRINCIPAUX.

2.3.I.I. TYPES DE DANGERS

Qu'il s'agisse d'informations (fichiers, données) ou de leurs traitements, quatre grands types de dangers se dégagent :

- perte d'enregistrements (disparition du fichier ou d'enregistrements à la suite de l'exécution d'un programme)
- modifications d'enregistrements ,
- destruction partielle ou totale d'enregistrements (écrasement d'enregistrements par d'autres, destruction des liens de chaînage, fonctionnement défectueux d'une tête de lecture/écriture),
- divulgation (lecture ou copie d'enregistrements non autorisés).

2.3.I.2. DEFINITION DES TERMES CONCERNANT LA SECURITE DES DONNEES.

Un des premiers problèmes rencontrés lorsqu'on parle de sécurité des données est la confusion des termes utilisés. Il est donc nécessaire, avant d'aller plus loin, de donner les définitions qui seront retenues dans le cadre de ce mémoire.

I. SECURITE (SECURITY)

Définition : Sécurité : terme que l'on peut évoquer chaque fois qu'il y a un risque de dégradation ou d'interruption des services ; il faudra minimiser la probabilité d'apparition du risque, c'est-à-dire la réduire à un niveau acceptable.

Pour un système informatique, celle-ci concerne :

- le personnel(opérateurs, programmeurs, l'administrateur de la base de données, le responsable de la sécurité, les techniciens, les analystes, etc...)
- les locaux qui abritent le système central contre les catastrophes accidentelles (feu, inondation) ou la malveillance ;
- l'alimentation électrique du système central (installation :
  - de dispositifs de protection contre les micro-coupures;
  - de groupes de secours autonomes à démarrage automatique en cas de "coupure zéro" ;
  - des stabilisateurs de tension..)
- le système central (dédoublement de matériels, voies d'accès multiples aux périphériques, dispositifs de commutation manuels ou télécommandés) ;
- les transmissions (plusieurs chemins de transmission, réseaux palmés ou soudés, arborescents ou en grappe qui permettent d'assurer le déroulement du trafic, même en cas d'interruption d'un des circuits.
- l'exploitation (règles, procédures qui diminuent les risques d'erreurs de pupitrage ou de manipulations de supports.)
- les informations (fichiers, programmes et documentation)

La sécurité des données est donc considérée comme un sous-ensemble de la sécurité au sens général.

Définition :.La "sécurité des données" (DATA SECURITY) concerne la sureté, la confidentialité des données contre une divulgation non autorisée, une modification ou une destruction, soit accidentelle, soit intentionnelle.

Celle-ci concerne :

.Les fichiers ordinateur et manuels.

REMARQUE : Dans le cadre de mémoire; on parlera de sécurité chaque fois qu'il y aura risque ;

(le tableau 2322 reprend tous les risques qui peuvent apparaître dans un système informatique ; le paragraphe 2.3.2.3. reprend ceux relatifs à l'utilisation d'un système de télétraitement.)

- on parlera de protection quand il faudra assurer la sécurité ;

(les différentes formes de protection couvrent à la fois les aspects hardware, software, administratifs et légaux.

2. CONFIDENTIALITE.(Aspects législatif et politique)

. confidentiel, secret des données;
. PRIVACY, préservation de la vie privée, sauvegarde des libertés individuelles ;

Définition : . ces termes sont utilisés dans un contexte légal ou social ayant trait à des informations propres aux individus (problèmes de la sauvegarde des libertés individuelles) ou propres à l'entreprise (données confidentielles , fichiers clients, marketing....)

. ces dispositions légales ou sociales permettent aux individus et aux entreprises :

a) de contrôler la disponibilité des informations. (comment les informations sont-elles collectées et par qui ?)
b) de contrôler l'utilisation de ces informations. (comment et par qui sont-elles utilisées, modifiées ou corrigées ?)

A ce niveau, on parlera rarement de dispositifs technologiques de sauvegarde mais plutôt de lois et de codes de déontologie.

3. INTEGRITE (INTEGRITY)

a) pour les constructeurs :

Définition : . intégrité s'applique aux fonctions réalisées par par un système d'exploitation en matière de sécurité des données.

. exemple : - fonction de point de contrôle et de reprise (CHECKPOINT/RESTART), de recouvrement (RECOVERY)
- fonction d'"isolation" des programmes lors des mises à jour en accès partagé. (problème des deadlocks).

b) d'une façon générale :

. sera synonyme d'exactitude, de validité des données ;
. signifie que les dispositifs de protection hardware, software ainsi que leurs interfaces manuels, doivent opérer ensemble d'une manière cohérente.

. exemples en télé-traitement :- validité des données entrées (accuracy) par des contrôles du type : codes détecteurs d'erreurs, détection avec ou sans retransmission automatique, plusieurs retransmissions consécutives...

- maintien de la confidentialité des données par des procédures d'identification et d'autorisation des utilisateurs ;
- validité des données entrées au moyen par exemple de contrôle de vraisemblance, etc...
- non-destruction des données assurée par des procédures de recouvrement, d'isolation de programmes lors d'accès partagés etc...
- validité des programmes (pas d'erreurs de logique ou d'erreurs préméditées).

2.3.2. LEURS CAUSES PRINCIPALES .

2.3.2.I. TYPES DE CAUSES.

Il est possible de distinguer trois types de causes à ces dangers

. causes accidentelles ou fortuites (négligences involontaires le plus souvent) ;

. nuisances préméditées déclenchées par des amateurs (par jeu ou par intérêt);

. nuisances préméditées déclenchées par des professionnels.

2.3.2.I. PROBABILITE D'APPARITION DES RISQUES POUVANT SE PRODUIRE DANS UN SYSTEME INFORMATIQUE.

Voir Fig. 232I.

2.3.2.3. RISQUES DUS A L'UTILISATION D'UN SYSTEME DE TELETRAITEMENT.

Les réseaux actuels de télétraitement présentent de grandes difficultés au développement de la sécurité des systèmes et peu de difficultés à d'éventuels escrocs.

La nécessité de mettre en place des mesures de sécurité provient de la nature et de l'importance des risques rencontrés lors de l'utilisation d'un système de télétraitement.

Exemples :

I) Un utilisateur n'ayant pas accès au système peut essayer de pénétrer dans celui-ci sans autorisation:

- en examinant attentivement les manipulations d'autres personnes, au terminal, il peut apprendre comment utiliser le terminal pour pénétrer dans le système ; une fois dans le système, il peut, comme tout autre utilisateur autorisé, accéder à n'importe quel programme ou donnée ;
- en formant le numéro de téléphone de l'ordinateur (numéro obtenu comme dans le cas précédent) ; une fois dans le système, celui-ci peut parfois fournir des instructions sur la façon de l'utiliser ;

Fig. 2321. PROBABILITE D'APPARITION DES RISQUES.

I. ACCIDENTEL	Destruction	Modification	Divulgation
a) événements "naturels"			
- feu, inondation, autres cataclysmes,	2		
- guerre.	2		
b) carences logiciel-hardware			
- panne machine (CPU),	5		
- piste de disque endommagée,	3 à 4		
- partie de bande magnétique endommagée,	3 à 4		
- volume magnétique illisible,	3		
- erreur logiciel-matériel endommageant un fichier,	4	5	
- erreur de transmission de donnée non détectée,	4	6	
- support d'entrée (ex. : cartes) détruit par la machine,	6	5	
- erreur programme application endommageant un fichier.	4	5	
2. NEGLIGEANCE HUMAINE (sans préméditation)			
- erreur saisie,	4	7	
- manipulations à partir de terminaux,	5	7	
- erreur pupitreur,	4	5 à 7	
- montage d'un volume inadéquat,		3 à 7	
- utilisation d'une version erronée d'un programme,		3 à 7	
- accident durant essais programme,	4	4 à 7	
- volume magnétique égaré,	3		2
- dommage physique sur un volume magnétique.	3		
3. AGRESSION HUMAINE (individuelle et préméditée)			
- pillage,	2		2
- sabotage violent,	2		
- sabotage non violent (effacement fichier)	2		
- erreur pupitreur,	3	3	
- erreur programmeur,	3	3	
- erreur bibliothécaire,	2		3
- erreur opérateur sur terminal,	3	3	
- erreur utilisateur,	3	3	
- erreur par jeu.	3	3	3
4. AGRESSION HUMAINE (collective et préméditée)			
- espionnage industriel,			4
- personnel vendant des secrets commerciaux,			3
- extorsion d'informations pour corruption ou chantage.			3

- CODIFICATION : 1. Probabilité d'apparition 1 fois tous les 400 ans,
  2. ..... 40 ans,
  3. ..... 4 ans,
  4. ..... 100 jours,
  5. ..... 10 jours,
  6. Probabilité d'apparition 1 fois/j.
  7. ..... 10 fois/J.

- au moyen d'un terminal non-autorisé, de codes ou de numéros d'identification appartenant à d'autres utilisateurs, en pénétrant dans le local où sont situés les terminaux réservés aux manipulations de données confidentielles ;
- en réintroduisant les commandes utilisées par un autre utilisateur (listing des manipulations abandonné dans une poubelle ou oublié au terminal, mots de passe apparaissant sur l'écran de visualisation lors de son introduction par un autre utilisateur);
- en se connectant à une ligne commutée (switched line) au moyen d'un terminal et d'un coupleur acoustique ; il peut non seulement lire des données, mais aussi bloquer l'autre terminal.

2) Un utilisateur non-autorisé à lire ou à modifier certaines informations peut obtenir celles-ci en interrogeant judicieusement la base de données :

- en demandant quel est le salaire le plus élevé dans son service, il peut connaître celui du chef de service ; (voir le problème des bases de données statistiques) ;

3) La plupart des tentatives accidentelles ou délibérées d'accès au système entraînent la divulgation de données à des personnes non-habilitées ; une destruction ou une divulgation accidentelle ont les mêmes conséquences que si elles étaient intentionnelles. De ce fait, les dispositifs de sauvegarde développés pour éviter les destructions accidentelles serviront aussi à éviter les agressions délibérées et vice-versa.

L'ensemble des risques dus à l'utilisation d'un système de télétraitement conduit à l'analyse des différentes formes de protection des bases de données. Avant d'aborder celles-ci en détail, (chapitre 2.) il semble nécessaire d'examiner brièvement l'attitude à prendre face aux risques.

2.3.2.4. PRINCIPES METHODOLOGIQUES.

Les principes méthodologiques retenus ici définissent l'attitude à prendre face aux risques décrits précédemment.

A. De façon générale, chaque danger doit être examiné sous trois axes :

I) Minimiser la probabilité d'apparition du risque :

. Dans tous les cas, il faut essayer de décourager les tentatives de fraude ou de malversation.
Exemples : . afin d'éviter les sabotages ou les fraudes programmées, il est souhaitable qu'au moins deux personnes travaillent au même projet ;

. changement périodique des mots de passe, réalisé automatiquement par l'ordinateur.

2. Minimiser les dommages quand l'incident se produit :

   Exemple : . un disque endommagé ou ne présentant plus une surface très plane doit être retiré car il risque d'endommager une tête de lecture, celle-ci pouvant endommager, à son tour, d'autres disques ;

3. Concevoir un dispositif pour redémarrer après l'incident ;

   Exemple : . si une personne entre en possession d'un code sécurité ou d'un fichier renfermant les codes sécurité de l'installation, il faut pouvoir modifier ceux-ci immédiatement en temps réel de telle sorte que les anciens soient inopérants.

   Remarques : - Ces axes d'étude couramment développés à propos du risque incendie sont souvent négligés pour les autres risques. Dans le cadre de ce mémoire, seuls les dangers provenant de manipulations à partir de terminaux seront évoqués.

   - Nous développerons plus loin une méthodologie de la mise en place d'un système de sécurité des données. (voir chapitre II, section 8)

B. Analyse d'opportunité.

Comme la sécurité des données, dans un système de télétraitement, comporte des aspects très divers qui peuvent conduire à des dépenses non négligeables en matériel et même en software (les différentes formes de protection couvrant à la fois les aspects techniques, administratifs, législatifs et politiques), il sera nécessaire d'apprécier toutes les composantes du coût de mise en oeuvre. Nous verrons que le niveau de sécurité désirable doit s'exprimer avec une connaissance claire des conséquences sur les solutions et les investissements.

CHAPITRE 2 :
avantages et inconvénients des techniques assurant la sécurité des données (non-pénétration et sauvegarde de l'intégrité)

section 1 : techniques de pénétration.

I.I. INTRODUCTION

Les banques de données contiennent des informations que les sociétés veulent maintenir confidentielles plus une gamme étendue d'informations personnelles sur la vie privée des individus (famille, études entreprises, dossier médical...)
Garder de telles informations hors de portée de personnes non habilitées est extrêmement important ; il sera donc nécessaire de les empêcher de lire des informations qui ne les concernent pas, de modifier des données, de créer ou de supprimer des enregistrements.

Or, on peut affirmer qu'il est actuellement possible de pénétrer dans n'importe quel système de télétraitement et d'outrepasser son dispositif de protection et de cette façon, d'accéder à toutes les ressources (mémoires, programmes, données) du système. Comme ces ressources sont partagées entre plusieurs utilisateurs, la confidentialité et l'intégrité des données sont gravement menacées.

Il s'avère donc indispensable de concevoir des dispositifs de protection hardware et/ou software efficaces. Avant d'aborder la synthèse des dispositifs existants ou faisant encore l'objet de recherches, (section 3 à 7) il convient de justifier l'affirmation donnée ci-dessus, en examinant les techniques de pénétration dans un système de télétraitement soi-disant protégé.

I.2. TECHNIQUES DE PENETRATION JUSTIFIANT LA MISE EN PLACE D'UN SYSTEME DE CONTROLE D'ACCES EFFICACE.

Outre les tentatives de pénétration décrites précédemment (CH. I 2323) et qui peuvent être perpétrées par des utilisateurs non-informaticiens, on peut considérer bien d'autres techniques de pénétration dues au fait que l'utilisateur du terminal est un spécialiste ou qu'il peut avoir étudié les dispositifs de protection soit, dans des brochures, soit, en essayant de découvrir des commandes non publiées dans ces brochures en entrant successivement des commandes erronées, ou encore en entrant des mots de passe utilisés sur un système analogue, etc...

I.2.I. PASSAGE EN ETAT "SUPERVISEUR" (ou "MASTER" mode).

Le but de l'utilisateur du terminal est, tout d'abord, de passer de l'état "problème" ("SLAVE" mode) à l'état "superviseur" où il n'existe aucune protection. ("MASTER" mode).

Pour des raisons évidentes, les utilisateurs n'ont jamais accès aux blocs de contrôle du système qui décrivent l'état des différents processus en cours. Si un utilisateur arrive à modifier les informations de ces blocs de contrôle, il peut, dès lors, usurper les contrôles du système d'exploitation.
La demande d'un checkpoint du programme utilisateur per_met, par exemple, d'avoir accès à ces blocs de contrôle. Cette opération a pour but de sauver, sur bande ou sur disque, des informations telles que les blocs de contrôle du programme.

L'utilisateur peut alors modifier les blocs dans le fichier des checkpoints et demander ensuite un restart de son programme.
Au redémarrage, son programme sera en état superviseur. Dès lors, il pourra accéder à toutes les ressources du système.

I.2.2. EXPLOITATION DES CARACTERISTIQUES DES SYSTEMES D'EXPLOITATION.

Une autre technique de pénétration consiste à exploiter le fait que, dans les opérating systems actuels, une partie du système dépend d'une autre partie pour valider ses entrées.

Exemple : Prenons l'exemple du relieur et du chargeur d'un système d'exploitation actuel : le chargeur suppose que les données (load module) provenant du relieur, sont exactes. Or, en modifiant quelque peu les sorties du relieur, un utilisateur peut amener le chargeur à recouvrir une partie du système avec son programme qui travaillera alors en état superviseur.

I.2.3. UTILISATION DU MECANISME DES INTERRUPTIONS.

Cette technique se base sur le fait que le système n'est pas protégé pendant la durée du traitement d'une interruption.

I.2.4. MISE A PROFIT DES FAIBLESSES DES SYSTEMES D'EXPLOITATION.

La plupart des systèmes ne font pas une remise à blancs ou à zéros des zones de mémoire (mémoire centrale ou auxilière) après l'exécution d'un programme. Des données résiduelles telles que des informations confidentielles ou des listes de mots de passe peuvent donc y subsister et être accessibles aux programmes suivants.

I.2.5. ENTREES NON CONTROLEES.

Certaines entrées dans le système sont intentionnellement dépourvues de dispositifs de contrôle : ex : routines, réservées aux programmeurs système. En général, celles-ci pourront être utilisées pour pénétrer dans le système en outrepassant les procédures de contrôle.

I.2.6. CONCLUSIONS.

S'il existe un seul point faible dans un système de sécurité, celui-ci pourra être utilisé pour pénétrer dans le système.

Exemple : Si un module n'est pas protégé, alors que tous les autres le sont, il pourra toujours être utilisé comme moyen de pénétration.

La sécurité des données, dans un système de télétraitement, nécessite le développement de techniques, méthodes, et procédures appropriées de protcction des informations contre les destructions, divulgations, ou modifications accidentelles ou délibérées des données.

L'établissement d'un système de sécurité repose sur trois parties :

1. Identifier les utilisateurs du système ;
2. Prévoir des mécanismes de protection pour empêcher toute entrée illégale dans le système et tout accès non autorisé aux fichiers;
3. Notifier au responsable de la sécurité (ou à une autorité équivalente) toutes tentatives de violation du système.

section 2 : description du processus de limitation de l'accès à des personnes autorisées.

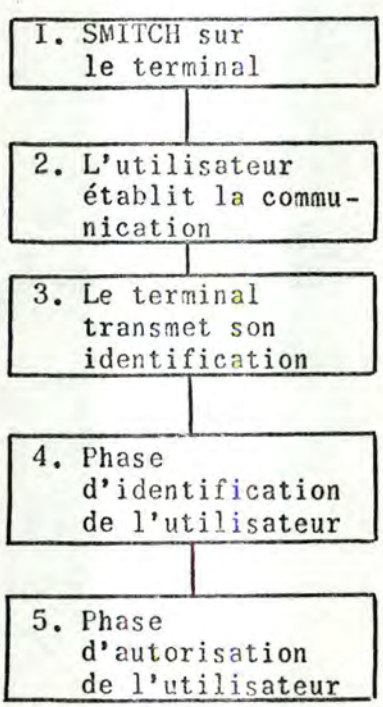
2.I. INTRODUCTION

Si nous considérons un système de télétraitement qui comporte un ou plusieurs processeurs, une hiérarchie de mémoires associées, un ensemble de fichiers d'informations (disques, tambours ou bandes), un réseau de communications ainsi qu'un ensemble de terminaux éloignés (reliés au système par des lignes louées ou commutées), le diagramme repris ci-dessous indique une séquence possible d'événements lorsqu'une personne utilise un terminal et un ensemble de transactions pour exécuter un ou plusieurs programmes à partir d'informations stockées dans une base de données.

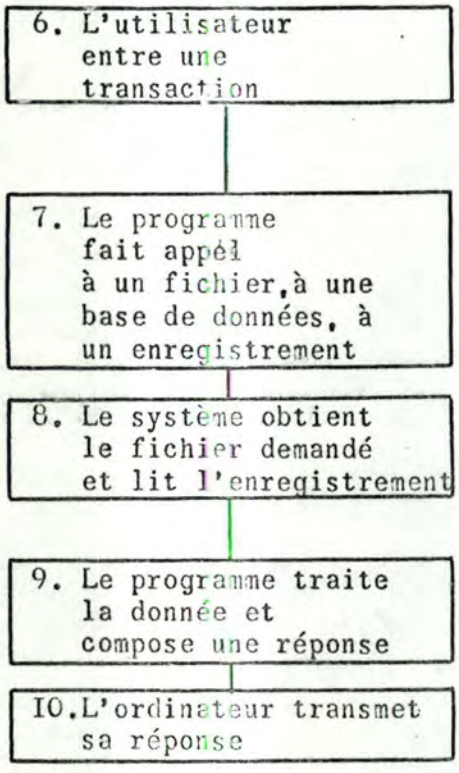
Les verrouillages qui peuvent être appliqués aux différentes étapes de la procédure ne doivent pas nécessairement être tous utilisés. Cependant, un système relativement sûr devrait comporter plus d'un verrouillage dans la chaîne, de telle sorte que si l'un d'entre eux est outrepassé accidentellement ou délibérément, les données soient toujours en sécurité.

2.2. DIAGRAMME DES EVENEMENTS RELATIFS A UNE SESSION DE TERMINAL.

EXEMPLE DE VERROUILLAGES POSSIBLES.



- Contrôle d'accès à la salle des terminaux; blocage du terminal; entre chaque session, par une clé physique.
- déconnextion du multiplexeur ou du concentrateur entre les heures normales de service; numéro de téléphone secret.
- Si le code d'identification (adresse) du terminal n'est pas accepté par l'ordinateur, toute transmission ultérieure sera bloquée.
- Le numéro d'identification de l'utilisateur peut ne pas être repris dans les tables du système : dans ce cas, aucune entrée ne sera acceptée.
- Contrôle du code sécurité (code secret, mot de passe, numéro ou clé...) selon les informations préalablement mémorisées dans les tables de sécurité du système.



- La librairie des programmes peut être protégée : l'utilisateur peut se voir refuser l'accès au programme qu'il a demandé explicitement, ou implicitement par une structure de dialogue.
- L'utilisateur (donc le programme) n'est pas autorisé à lire ou à modifier le fichier ou l'enregistrement : l'accès à ceux-ci sera inhibé.
- L'enregistrement ou l'item demandé contient un indicateur interdisant à cet utilisateur de le lire ou de le le modifier.
- Dans certains cas, l'inhibition d'une réponse à l'utilisateur peut dépendre du résultat du traitement de la donnée.
- Comme l'information n'est susceptible d'apparaître confidentielle qu'après la réalisation de certains traitements; le programme d'application peut avoir son propre mécanisme pour empêcher la divulgation du résultat.

Tous les systèmes de protection décrits soit, dans la littérature actuelle, soit, chez les constructeurs et pouvant s'appliquer aux événements I à 8 seront détaillés dans les sections qui suivent.

On abordera notamment les problèmes d'identification, d'autorisation, de concurrence entre programmes, de PRIVACY (lois) et de personnel (rédaction des programmes, vérification).

On développera, au chapitre III, un programme de contrôle d'accès basé sur l'enchaînement des événements I à 8. Les événements 9 et 10 ne seront pas abordés puisqu'ils dépendent de chaque programme d'application.

Le chapitre IV donnera les principales directives suivies pour implémenter le programme de contrôle d'accès élaboré au chapitre III. On trouvera, en fin de chapitre, les résultats de l'implémentation du programme réalisé au cours d'un stage à l'IBM Belgium.

section 3 : contrôle des accès aux terminaux et à chaque terminal en particulier

3.I. TERMINAUX AVEC ET SANS DISPOSITIF DE PROTECTION

On peut considérer deux types de terminaux :

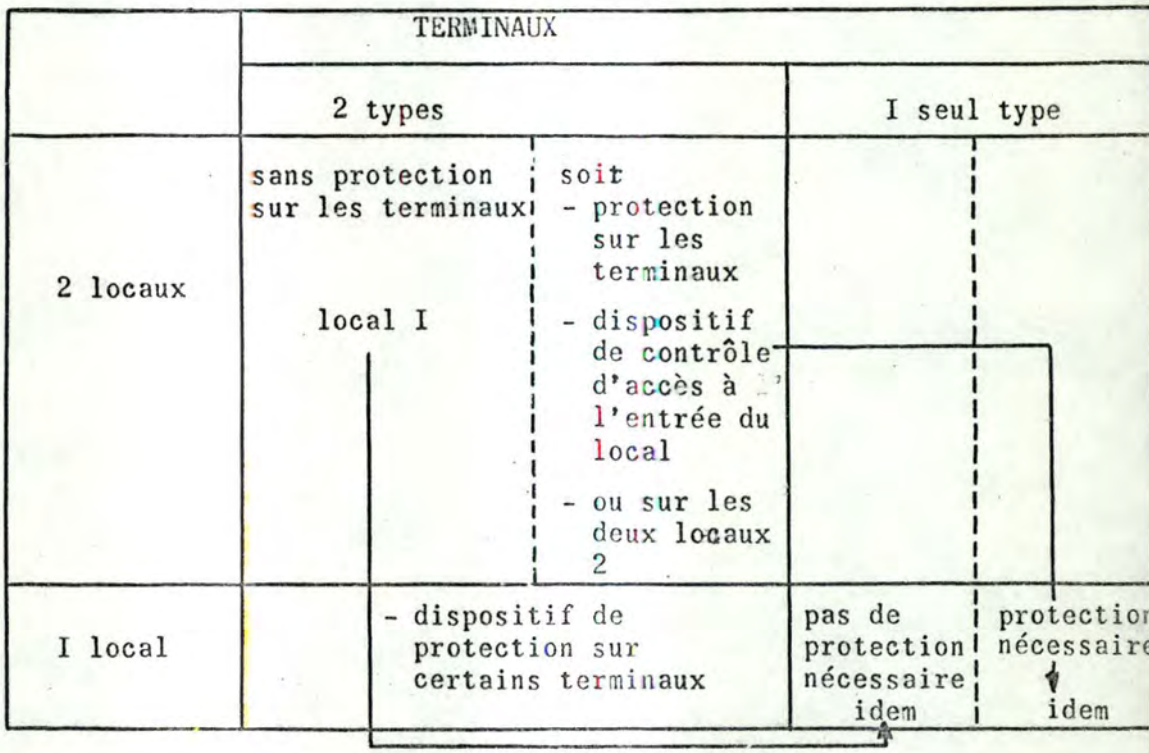
- . avec protection : donc non accessibles par tous les utilisateurs
- . sans protection : accessibles théoriquement par tous les utilisateurs.

Si les deux types de terminaux sont admis, il est souhaitable de les placer dans des locaux différents : ceci permettra d'éviter qu'un personne non autorisée à travailler sur un terminal protégé examine les manipulations d'une personne habilitée.

- . exemple de manipulations :
  - entrée d'un code sécurité,
  - entrée d'informations confidentielles.
- . risques encourus par la personne habilitée :

  Exemple : cas d'un terminal à écran cathodique.
  - rique qu'un observateur remarque le code de sécurité employé lors de son introduction au clavier (touches utilisées), même si ce code n'apparaît pas sur l'écran,
  - risque d'oublier de retirer sa clé (physique) dans la serrure sur le terminal,
  - risque qu'un observateur remarque des données confidentiel les, soit, sur l'écran, soit, sur les documents de travail de l'opérateur,
  - risque, pour les terminaux avec imprimante, d'oublier un listing contenant l'enchaînement de manipulations (commandes d'identification de l'opérateur ; ce listing pouvant être abandonné sur l'imprimante ou dans la poubelle (et oui) à la suite d'erreurs de manipulation.

Ceci nous amène à considérer une ou deux zones d'implantation des terminaux. Suivant le cas, les dispositifs de protection mis en place seront différents :



3.2. PROTECTION DU TERMINAL.

Un terminal peut être équipé :

. d'une serrure

Exemples :

- un agent de banque peut avoir sa propre clé ; chaque fois qu'il entre une transaction, il doit insérer cette clé dans la serrure du terminal afin de débloquer le clavier.
- certains terminaux bancaires ont même deux serrures, de telle sorte que deux caissiers séparés puissent l'utiliser.

Inconvénients :

- risque de perdre la clé ; multiplication du nombre de serrures sur le terminal si chaque utilisateur doit avoir une clé unique ; baisse de l'efficacité du système de protection si tous les utilisateurs ont une clé identique.

. d'un lecteur de cartes d'identification : la carte a la dimension d'une carte de crédit et contient des données sur une piste magnétique.

Exemples d'utilisation :

- voir paragraphe suivant et section 5.

Avantages :

- la carte magnétique est la clé d'un système de contrôle d'accès ;
- elle possède un code invisible, insensible aux agents extérieurs (humidité par exemple) ;
- un très grand nombre de codes différents peuvent être composés, assurant ainsi à chaque carte un code unique, renouvelable et programmable.
- la carte peut être imprimée au nom, à l'adresse du propriétaire. Sa photographie peut apparaître au verso de la carte.

Remarque : à ce stade, la carte magnétique sert de clé au système de contrôle d'accès du terminal : si les données de la piste magnétique sont reconnues valides, le terminal pourra, par exemple, être mis sous tension, le clavier sera débloqué; l'opérateur pourra former le numéro de téléphone de l'ordinateur ; les mêmes données pourront ensuite être utilisées par une routine de contrôle d'accès (voir programme développé au chapitre 3) pour identifier l'utilisateur du terminal. La carte magnétique peut aussi être utilisée a l'entrée de la salle des terminaux.

3.3. PROTECTION DE LA SALLE DES TERMINAUX.

Il existe actuellement, parmi la multitude des dispositifs de contrôle d'accès, certains dispositifs très évolués présentant un caractère modulaire et pouvant s'adapter au degré de sécurité retenu pour le problème posé.

On peut les classer en trois catégories :

- les dispositifs qui utilisent une carte magnétique et/ou une clé,
- ceux à commande électronique où la clé est remplacée par un système de code,
- ceux qui combinent les deux dispositifs précédents.

3.3.I. DISPOSITIF SELECTEUR (degré de sécurité n° I)

C'est le cas d'utilisation le plus simple. Deux éléments de contrôle sont utilisés :

- une carte magnétique codée,
- un sélecteur qui accepte ou refuse la carte proposée et commande soit l'ouverture de portes, soit la mise en service de machines.

Avantages :

- une carte peut être codée de façon à donner accès à un ou plusieurs sélecteurs à la fois.
- pour qu'une carte soit acceptée, il faut que son code soit conforme à celui d'une matrice placée à l'intérieur de l'appareil ; dans le cas contraire, le sélecteur la refuse.
- un système de codage double permet l'accès à certaines heures seulement.(équipe de nuit et de jour, par exemple.)
- possibilité de codes illimitée.

Inconvénients :

- risque de perte ou de prêt abusif des cartes.

Solution :

- Pour limiter un prêt abusif des cartes entre différentes personnes, la firme Fichet-Bauche a commercialisé un système "I.R." (Invalideur-Revalideur) qui peut être adapté au sélecteur :

  . après une entrée autorisée, l'invalideur efface automatiquement certaines informations sur la carte, informations qui sont restituées au poste de sortie où le revalideur la programme de nouveau pour une autre entrée.

3.3.2. CENTRALE DE CONTROLE AVEC LECTEUR DE CARTES (degré de sécurité n°2)

Le système de contrôle d'accès comprend un lecteur de cartes magnétiques individuelles à double code :

- le premier permet de vérifier si la carte a été codée pour être lue par le lecteur. Si cette condition est remplie, le second code de la carte est transmis en code binaire à une centrale de contrôle. Le code de la carte est vérifié et si sa validité est reconnue, l'autorisation d'accès est accordée.

Avantages :

- Pour chaque présentation de la carte, la centrale imprime le jour, l'heure, la minute, le numéro de la porte et le code de la carte. Elle indique, de plus, si l'accès a été accordé ou refusé. (Dans ce dernier cas, la centrale peut actionner un système d'alarme).

Remarque :

- Le système le plus évolué est piloté par un mini-ordinateur (centrale). Celui-ci accorde ou non l'entrée en fonction de sa programmation et enregistre sur imprimante, bande perforée ou magnétique, tous les passages des usagers aux différentes portes ou points d'accès. Toute carte perdue, volée ou conservée par l'utilisateur peut être immédiatement annulée.

  Exemple : Système des cartes-clés SAFAA.

3.3.3. BLOCS DE LECTURE (degré de sécurité n° 3) A CODAGE NUMERIQUE OU ALPHABETIQUE.

Une protection plus importante peut être obtenue à partir de ce système qui comporte généralement :

- un clavier à IO ou I5 touches sur lequel il faut établir une combinaison et un lecteur de cartes magnétiques,
- une armoire de contrôle fait partie de chaque ensemble.

Exemples : (blocs de lecture M.L. de la firme Fichet-Bauche).

- l'entrée dans un local s'effectue après l'introduction de la carte dans le lecteur et affichage d'une combinaison de 3 chiffres ou 3 lettres (suivant le bloc de lecture prévu).
  - . l'introduction de la carte peut être programmée pour s'effectuer au début, à la fin de l'opération ou entre la frappe des deux chiffres ou lettres du code.
  - . Exemple : 3-8 - introduction de la carte - 5.
- une alarme, dite de contrainte est prévue dans ce système :
  - . dans ce cas, il suffit de frapper une touche déterminée à l'avance, à la place du dernier chiffre (ou lettre) du code habituel.
- lors de l'établissement de la combinaison sur les blocs de lecture, un nombre d'erreurs, réglable de I à 9, est admis. Passé ce nombre, une alarme se déclenche automatiquement.

Remarque :

Ces blocs de lecture peuvent fonctionner d'une manière autonome ou être équipés d'un lecteur de cartes relié à une centrale qui contrôle les informations de la carte et autorise ou refuse l'accès demandé. (voir 3.2.2.2).

Si on désire un degré de sécurité plus élevé, chaque carte magnétique possèdera son propre code (au lieu d'un même code pour toutes les personnes possédant une carte). En général, une erreur de code bloque le système pendant une durée réglable (I à 30 sec. par exemple).

Le dispositif : . donne l'alarme après une ou plusieurs erreurs de code;
. possède un dispositif d'autoprotection en cas d'ouverture du boitier.

3.3.4. SCHEMA DE FONCTIONNEMENT D'UN BLOC DE LECTURE A CODAGE NUMERIQUE.

Nous prendrons comme exemple, ici, le terminal TCA II2I. de la firme française EIPROS. (Spécialisée dans les terminaux légers qui transforment le poste téléphonique en périphérique d'ordinateur.) Le TCA II2I se raccorde aux ordinateurs par l'intermédiaire d'autocommutateurs électroniques multifréquences.

Ce terminal de contrôle d'accès est un lecteur de badge raccordé à une ligne téléphonique permettant la transmission d'informations contenues sur ce dit badge et d'informations introduites sur un clavier de I2 touches. La lecture du badge peut être interrompue par l'introduction d'informations au clavier. Le schéma de la Fig. 3.3.4. indique un moyen de résoudre tous les problèmes d'un dispositif de contrôle d'accès évolué.

I) Présentation du terminal :

Ce terminal est présenté dans un boîtier et comporte :
- une entrée badge,
- un voyant rouge (tonalité discontinue),
- un voyant vert (commande d'ouverture),
- un bouton "start", quatre de sélection : "in", "out", "service", "CL", ainsi qu'un clavier à I2 touches.
- une entrée ligne téléphonique.

2) Fonctionnement :

I) Entrée du badge (badge perforé : 22 colonnes/I2 lignes)

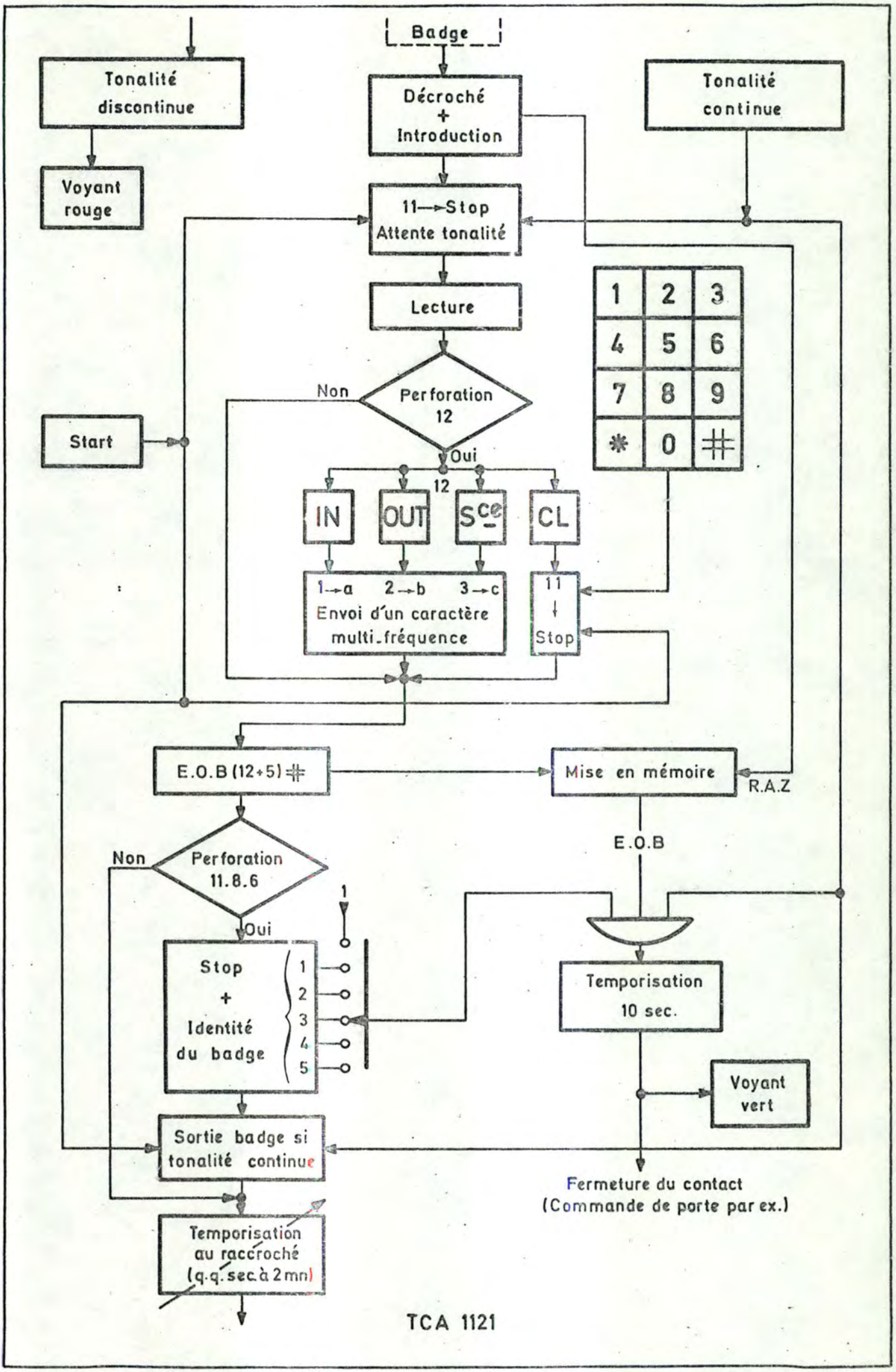
- Le "décroché" est obtenu dès l'introduction du badge.
- En présence d'une perforation II :
  - . si la tonalité est continue : la lecture est enclenchée;
  - . si la tonalité est discontinue : agir sur "Start" et recommencer.

2) Lecture du badge :

- Présence d'une perforation en colonne I2 :
  - . touches "in", "out" ou "Service" enfoncées :
    - envoi d'une information multifréquence ;
  - . touche "CL" enfoncée :
    - la lecture du badge est arrêtée et le clavier est mis en fonction ; introduction de données variables.
    - la lecture du badge sera poursuivie par l'action sur le bouton "start".
- Perforation I2 inexistante ; la lecture du badge se poursuit jusqu'à l'apparition du "End of Block" (I2-5); ce dernier est mis en mémoire.

3) Identification du badge par rapport au lecteur :

- Présence des perforations II-8-6 et 1 ou 2 ou 3 ou 4 ou 5 : (supposons que le lecteur soit repéré en position 3)
  - . le badge est stoppé ;
  - . à l'apparition de la tonalité continue, un contact de commande est actionné (voyant vert) pendant I0 secondes environ et le badge est extrait.(si3ds le badge);
  - . si le badge ne comporte que les perforations II-8-6 la présence de la tonalité n'actionnera pas le contact de commande.
  - . remarquons que si le badge comporte plusieurs perforations (dans les lignes I, 2; 3, 4 ou 5), il pourra être utilisé sur plusieurs lecteurs répérés conformément au badge.
- S'il n'y a pas de perforations d'identification et que le lecteur n'est pas repéré, le badge est extrait et le contact de commande est actionné dès la présence de la tonalité continue.


Badge
Tonalité discontinue
Décroché + Introduction
Tonalité continue
Voyant rouge
11→Stop Attente tonalité
Lecture
1 2 3
4 5 6
7 8 9
* 0 #
Non
Perforation 12
Start
Oui
12
IN
OUT
Sce
CL
1→a 2→b 3→c
Envoi d'un caractère multi-fréquence
11
Stop
E.O.B (12+5) #
Mise en mémoire
R.A.Z
E.O.B
Non
Perforation 11.8.6
Oui
1
Stop + Identité du badge
1
2
3
4
5
Temporisation 10 sec.
Voyant vert
Sortie badge si tonalité continue
Fermeture du contact
(Commande de porte par ex.)
Temporisation au raccroché (q.q. sec. à 2 mn)
TCA 1121

3.3. ETABLISSEMENT DE LA COMMUNICATION.

Les procédures de communication peuvent être bloquées, (le soir, pendant les périodes d'entretien, congés etc...)pour éviter tout accès interdit, en déconnectant par exemple :

. le multiplexeur ou le concentrateur,

. les modems (serrure physique sur le modem).

Le numéro de téléphone pour entrer en communication avec l'ordinateur sera tenu secret et ne pourra, en aucun cas, figurer sur un annuaire.

3.4. REMARQUE.

Dès que l'utilisateur a accès à la salle des terminaux et à un terminal en particulier, il peut établir la communication. L'ordinateur doit alors pouvoir identifier le terminal qui demande la communication, ainsi que l'utilisateur de ce terminal. Ceci nécessitera des procédures spéciales et des dispositifs de contrôle d'accès semblables à ceux-ci.

section 4 : identification du terminal.

4.I. CHOIX DE LA PROCEDURE D'IDENTIFICATION.

Sur certains systèmes, il sera nécessaire d'identifier à la fois le terminal et l'utilisateur ou l'opérateur de ce terminal. Sur d'autres systèmes, une seule identification suffira. Différentes raisons permettent de faire un choix entre les deux procédures ou de les appliquer toutes deux.

4.I.I. IDENTIFICATION DU TERMINAL UNIQUEMENT :

Si les terminaux sont répartis dans deux locaux différents, ceux dont il faut assurer la protection seront placés dans le local (ou zone) dit "de sécurité". Leur protection sera assurée par un dispositif de limitation de l'accès placé à l'entrée du local (voir section 2) et cette protection peut être considérée comme suffisante.
Pour l'ordinateur, la procédure de sécurité consistera à s'assurer qu'il est bien en communication avec ses terminaux.

La Fig. 4.I. illustre cette situation : l'installation comprend :

- un concentrateur (ou une unité de contrôle),
- des terminaux sans sécurité et d'autres implantés dans une zone dite "de sécurité".

4.I.2. IDENTIFICATION DE L'UTILISATEUR UNIQUEMENT :

Certains systèmes contenant des données confidentielles se basent sur des techniques d'identification de l'utilisateur (voir section 5) plutôt que du terminal ou de son emplacement, ce qui permet, lorsqu'un terminal tombe en panne, de rapidement l'interchanger avec un autre.

4.I.3. REMARQUE :

Il est toujours possible de combiner les deux procédures décrites ci-dessus si l'on désire un degré de sécurité plus important. En pratique, le côût sera un facteur limitatif pour toutes les opérations éventuelles qui pourraient être apportées en vue de renforcer l'efficacité du système de sécurité.

4.2. TECHNIQUES D'IDENTIFICATION DU TERMINAL.

4.2.I. PAR ADRESSE

A. Principe :

Pour des raisons d'économie de ligne, des terminaux protégés (réservés pour l'introduction de données confidentielles) partagent souvent des lignes de communication avec des terminaux non protégés. (Fig. 4.I).

Par conséquent, l'ordinateur doit connaître l'adresse du terminal avec lequel il est entré en communication. Il suffit que cette adresse précède chaque message envoyé par le terminal (voir cours de télétraitement de 2° licence).

B. Fonctionnement :

L'ordinateur peut interroger, par exemple, un terminal au moyen d'une adresse spécifique. Même lorsqu'une interrogation générale est envoyée à une unité de contrôle, pour laquelle n'importe quel terminal peut répondre, l'ordinateur connait toujours le terminal répondant, puisque son adresse précède le message de réponse. Le système parcourt alors une table qui lui indique, pour chaque adresse de terminal, s'il doit la traiter avec ou sans sécurité.

C. Remarque :

Sur certains systèmes, une personne non autorisée qui désirerait avoir accès au système peut intervertir les adresses des terminaux. Ceci n'est possible qu'avec certaines configurations de ligne.

Exemple : Dans la configuration précédente (voir Fig. 4.I), le câble reliant l'unité de contrôle au terminal à écran cathodique peut être interchangé avec celui d'un autre terminal. L'ordinateur va, dès lors, considérer (suivant la table des adresses des terminaux) le terminal de substitution comme étant dans la zone de sécurité. L'utilisateur pourra ainsi avoir accès à des données confidentielles.

L'interchangement des câbles de connection ne sera probablement pas réalisable si l'unité de contrôle est elle-même disposée dans la zone de sécurité. (voir Fig. 4.2.I)

4.2.2. PAR CODE DE SECURITE CABLE.

A. Principe :

Afin de protéger le système contre tout interchangement de terminaux, il est préférable de câbler un code de sécurité dans le hardware du terminal. Un changement de code est alors impossible sans une connaissance approfondie du système.

B. Exemple :

La Fig. 4.2.2. représente la structure du code d'identification du terminal IBM 2770, qui comprend deux parties câblées, l'une dépendant de l'utilisateur, l'autre du constructeur.

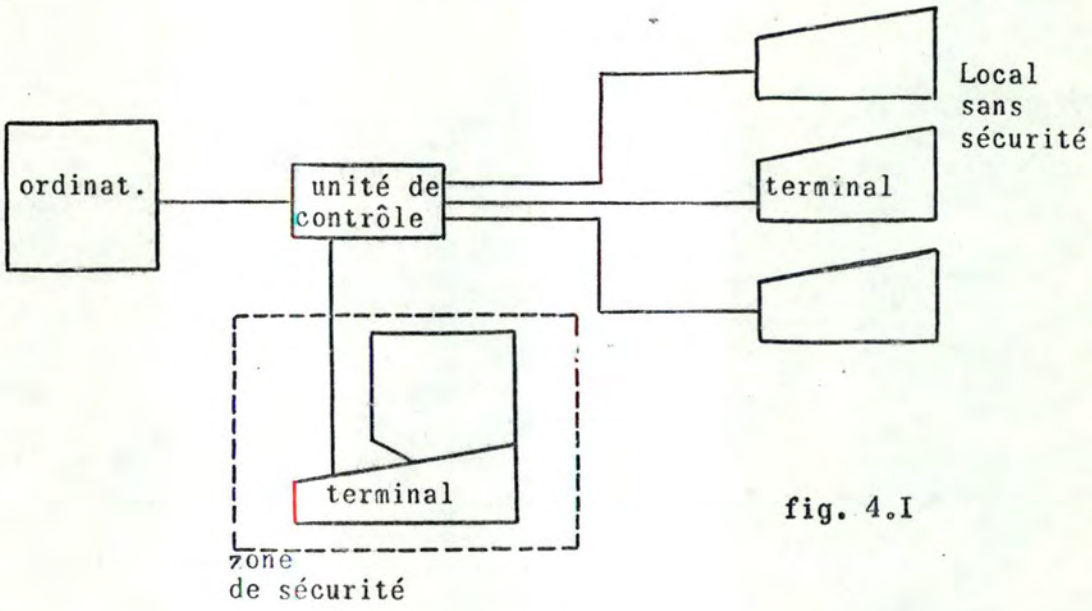


fig. 4.I

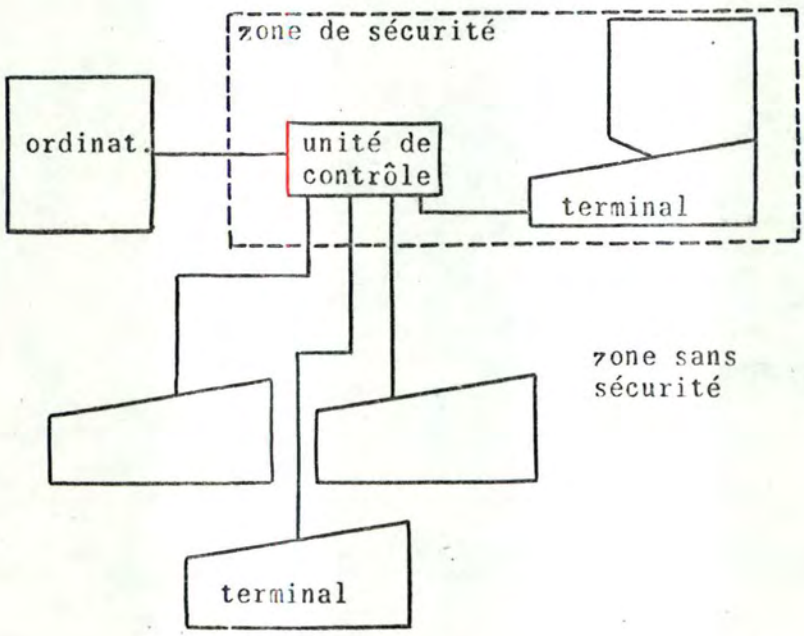


fig. 4.2.I

caractères de synchronisation

SYN	
SYN	
X	caractères d'identification
X	(câblés par un ingénieur de la firme de l'utilisateur)
A	caractères de sécurité
B	câblés dans le terminal dès sa fabrication
C	
ENQ	demande d'autorisation de transmettre

Structure du code d'identification du terminal IBM 2770

fig. 4.2.2

4.3. FREQUENCE D'IDENTIFICATION.

La fréquence selon laquelle les terminaux doivent s'identifier au système peut dépendre d'un ou plusieurs facteurs :

- programme en cours,
- risques (tentative d'accès non autorisée),
- probabilité de substitution d'un autre terminal,
- nombre de terminaux actifs,
- caractéristiques des terminaux.

D'une façon générale, l'identification se fera : soit

- automatiquement, lors de la première transmission ou de l'initialisation (SIGN-ON) de la session terminal ;
- lors de chaque message ;
- lorsqu'une interruption a été détectée par l'ordinateur (remarquons que le réseau téléphonique n'offre aucun moyen de détecter le remplacement du terminal pendant la durée de l'interruption.)

4.4. CONCLUSIONS.

On peut considérer deux niveaux d'identification :

- soit identifier le terminal sans fournir une protection contre des interchangements délibérés de terminaux ;
- soit fournir un code de sécurité câblé, rendant ainsi impossible tout interchangement ;

Le principal inconvénient de l'utilisation d'une technique d'identification du terminal réside dans la lenteur de la procédure de substitution en cas de panne de ce dernier.

Un utilisateur (autorisé) doit, tout d'abord, avertir le centre de traitement ;
Il faut, ensuite;
- substituer un nouveau terminal à celui qui est défectueux ;
- modifier les entrées correspondantes dans la table des terminaux.

La procédure de reprise du traitement sur un autre terminal n'est donc pas automatique aussi la plupart des systèmes traitant des données confidentielles préfèrent baser leur système de contrôle d'accès sur une identification de l'utilisateur plutôt que sur celle du terminal ou de son emplacement.

section 5 : identification de l'utilisateur.

5.I. INTRODUCTION.

Si la base de données ne contient pas d'informations confidentielles, l'identification du terminal sera suffisante ; par exemple, si tous les employés d'un même département peuvent accéder au fichier de leur département à partir d'un terminal, il suffira de disposer celui-ci dans ce département.

La situation du terminal peut donc fournir une protection suffisante.

Si, par contre, plusieurs utilisateurs partagent le même terminal et que des niveaux de confidentialité différents sont appliqués aux utilisateurs, il faudra non seulement identifier le terminal mais aussi l'utilisateur de celui-ci.
Ceci peut se faire de trois façons différentes :

1. Par une donnée que la personne connait ou qu'elle a mémorisé :

   Principe : La personne peut mémoriser un mot de passe, un nombre secret ou répondre à un ensemble prédéterminé de question

   Coût : Les techniciens de ce type n'exigent pas un hardware spécial : la procédure d'identification relève uniquement du software (programme d'identification). Elles sont les moins coûteuses et peuvent être réalisées pour assurer raisonnablement, mais non infailliblement, la sécurité.

2. Par un objet que la personne peut garder sur elle :

   Principe : Insertion d'un badge ou d'une carte dans un lecteur raccordé au terminal ou inclu dans celui-ci ou insertion d'une clé dans la serrure du terminal (voir précédemment section 2).

   Côut : Ces techniques nécessitent un dispositif hardware de lecture parfois très coûteux car n'étant pas encore inclus de façon standard, dans tous les terminaux.

3. Au moyen de caractéristiques physiques de la personne.

   Principe : Un dispositif pourrait être utilisé pour la lecture et la transmission de l'empreinte des doigts ou du pouce et comparée par un programme à des données pré-enregistrées. De plus, la voix pourrait être transmise à l'ordinateur : l'utilisateur prononce dans un ordre prédéterminé certaines syllabes que l'ordinateur compare ensuite à un enregistrement préalablement mémorisé. D'autres caractéristiques physiques pourraient également être utilisées.

coût : Actuellement, ces techniques font partie du domaine de la recherche. Celles-ci sont de loin les plus fiables mais aussi les plus coûteuses. Actuellement, un seul lecteur d'empreintes et un seul dispositif à entrée vocale ont été commercialisés.

5.2. IDENTIFICATION PAR UNE DONNEE QUE LA PERSONNE CONNAÎT OU QU'ELLE A MEMORISE.

5.2.1. PROTECTION PAR MOT DE PASSE/CLE/CODE SECURITE.

Les informations peuvent être protégées d'une façon peu coûteuse, l'ordinateur demandant à l'utilisateur de s'identifier par un mot de passe ou un code que lui seul connaît.

5.2.1.1. MOT DE PASSE UNIQUE, COMMUN A PLUSIEURS PERSONNES.

La procédure la plus simple est d'utiliser un seul mot de passe commun à toutes les personnes habilitées à employer le terminal. Le système n'admet aucune transaction tant qu'il n'a pas été introduit.

Principe : Sur beaucoup de systèmes en temps-partagé, l'opérateur du terminal crée et met à jour son propre fichier. Il lui fournit un mot de passe ou même plusieurs s'il en veut différentes parties. Ce fichier ne peut être lu par quiconque ne fournit pas le mot de passe correct. L'utilisateur du terminal est libre de changer, chaque fois qu'il le désire, le mot de passe avec lequel il a verrouillé son fichier.

Une procédure identique est utilisée aujourd'hui sur de nombreux systèmes de télétraitement et s'avère efficace pour ifentifier les utilisateurs qui voudraient accéder aux informations (programmes, données, utilitaires) à partir des terminaux. (voir section 6).

5.2.1.2. MOT DE PASSE OU CODE DE SECURITE INDIVIDUEL.

Afin d'établir un dispositif de protection plus efficace, il est préférable que chaque utilisateur du terminal ait un code différent.
Sur certains systèmes; l'utilisateur doit indiquer :

- son numéro personnel d'identification (ex : nom, numéro de matricule, numéro du registre national) ,
- son code de sécurité ou mot de passe.

L'ordinateur (routine d'identification) peut alors vérifier si le code sécurité est bien celui qui a été affecté à la personne qui a fourni le numéro d'identification.

Exemple : + USER NAME?
426,SMITH (numéro d'identification + nom)
+ PASSWORD?
NØBØDY44

5;2.I.3. INCONVENIENTS DES MOTS DE PASSE ET CODES DE SECURITE.

La plupart de ces procédures ne fournissent pas un haut degré de sécurité (tous les utilisateurs d'un fichier de données utilisent le même mot de passe). Dans certains cas, l'ensemble des mots de passe des fichiers ne sont pas protégés par un autre mot de passe.
L'utilisation de mots de passe ou de codes de sécurité présentent également d'autres inconvénients :

1. Les utilisateurs ne protègent pas leur mot de passe. Le code peut donc être donné à une autre personne ou observé par celle-ci.
   Rien ne met en évidence la personne qui est entrée en possession de ce code. De plus, comme beaucoup d'utilisateurs l'écrivent sur un calepin ou sur un bout de papier pour le retenir plus facilement, n'importe qui peut en prendre connaissance sans que l'on s'en aperçoive.
2. Les utilisateurs oublient leur mot de passe personnel ou leur code de sécurité.

   De plus, pour un même utilisateur, la probabilité d'oublier un mot de passe est proportionnelle à la fréquence de modification de celui-ci.

   En cas d'oubli, l'utilisateur devra prévenir l'opérateur du centre informatique. Celui-ci devra donc posséder une liste des différents mots de passe utilisés.

Ces inconvénients pourront facilement être évités si chaque mot de passe ou code sécurité est rendu invalide après sa première utilisation. (voir 5.2.I.6.)

5.2.I.4. REMARQUE :

A. MOT DE PASSE (MOT-CLE) :

- peut contenir toutes combinaisons de lettres, de chiffres ou de caractères spéciaux.

B. CODE SECURITE :

- en général, ne contient que des chiffres.

5.2.I.5. CHOIX ET GENERATION DES MOTS DE PASSES OU CODES SECURITE.

Règles :
1. Grand nombre de combinaisons possibles afin qu'une personne non autorisée à accéder au système ne trouve pas, par hasard une clé valide.
2. Le degré de sécurité obtenu est proportionnel à la longueur de la clé.
3. La clé doit pouvoir être sélectionnée au hasard parmi toutes les combinaisons.

4. La clé doit pouvoir être mémorisée facilement. (objectif contradictoire à la règle 2)

5. Chaque clé doit pouvoir être modifiée indépendamment de toutes les autres.

Une solution de compromis entre ces exigences sera de choisir une clé de trois lettres au hasard suivies de trois chiffres déterminés au hasard également.

Remarque : avantages d'une clé personnelle plutôt que d'une clé de groupe : (clé identique pour toutes les personnes d'un département.

- une personne peut changer de groupe sans devoir modifier la clé de ce dernier;
- il sera plus facile d'identifier un utilisateur non-autorisé ou essayant de forcer le dispositif de protection ;
- la modification d'une clé personnelle se remarquera moins que la modification de celle d'un groupe (si une personne non-autorisée remarque celle-ci lors d'une introduction par son propriétaire.

5.2.I.6. PERIODE DE VALIDITE.

Règle : Le degré de sécurité obtenu en utilisant un mot de passe ou un code sécurité est inversément proportionnel à sa durée d'utilisation.

Améliorations à la protection par mot de passe :

- changements périodiques ou imprévisibles,
- utilisation unique.

5.2.I.6.I. CHANGEMENTS PERIODIQUES OU IMPREVISIBLES.

Sur certains systèmes, les codes sont changés tous les mois. une modification imprévisible est préférable : comme la période de validité est indéterminée, toute personne non-autorisée qui posséderait un mot de passe, sera détectée dès la fin de la période de validité de celui-ci.

Procédure de modification :

- exemple : le nouveau code de sécurité est envoyé à chaque utilisateur lors de l'expédition de ses factures du mois. Le code se trouve sur une partie détachable ne comportant aucune autre mention. L'utilisateur est prié de détacher la partie comprenant le code sécurité et de ne le divulguer sous aucun prétexte. S'il perd cette carte, il est peu vraisemblable qu'une autre personne puisse l'associer au numéro d'identification correct.
- Remarque : L'utilisateur peut demander un nouveau code de sécurité ou mot de passe, chaque fois qu'il le désire : par exemple, s'il croit que quelqu'un l'a observé lorsqu'il l'introduisait au clavier.

5.2.I.6.2. MOTS DE PASSE, CODES SECURITE, NOMBRES SECRETS INVALIDES APRES LEUR PREMIERE UTILISATION.

Principe : Afin d'éviter qu'une autre personne puisse employer ultérieurement le mot de passe ou le code sécurité d'un utilisateur, ce code, une fois utilisé, deviendra invalide.
Dans un système de ce genre, l'utilisateur a la possibilité de renouveler son mot de passe à chaque session de terminal.

Différentes méthodes permettent d'annuler un mot de passe ou un code sécurité :

- liste de codes ou de mots de passe,
- nombres secrets et génération de nombres au hasard, avec : . transformation logique,
  . fonction algébrique.

A. Listes de codes ou de mots de passe.

Principe : Le responsable de la sécurité fournit à l'utilisateur une liste de codes plutôt qu'un seul. Il est invité à ne pas barrer sur sa liste les codes invalides ; une personne non-autorisée ne pourra utiliser cette carte, ne sachant pas quel est le code à introduire. (la période de validité peut aussi être la durée d'une transaction.)

B. Nombres secrets et génération de nombres au hasard.

Principe : l'utilisateur entre certains digits d'un nombre mémorisé. Chaque digit est déterminé, de manière aléatoire, par le système.

Description : Supposons que chaque utilisateur mémorise un nombre, un mot ou une phrase pouvant contenir n'importe quels caractères et facile à mémoriser, si bien qu'on permet à l'utilisateur de le composer lui-même.
Appelons ce nombre, un "nombre secret". Il sera différent du numéro d'identification de l'utilisateur afin :

. qu'il n'en existe aucune trace écrite ;
. d'éliminer toute possibilité qu'une autre personne entre en sa possession.

Exemple : Lors de la procédure d'identification, l'ordinateur demande à l'utilisateur de lui fournir certains caractères du nombre secret (soit une paire ≠ à chaque identification). Le dialogue d'identification sera par exemple :

```
6TYPE YOUR SECURITY CODE
/00002344
+TYPE THE FIRST AND SEVENTH CHARACTERS
+SECRET NUMBER                    OF YOUR
/X3
+PROCEED
```

C. Méthodes dérivées de l'emploi de la technique des nombres au hasard.

Principe : L'ordinateur fournit d'abord un nombre pseudo-aléatoire à l'utilisateur; celui-ci exécute ensuite une

transformation logique ou mathématique (règles prédéterminées) et renvoie le nombre résultant de cette transformation, (mot de passe) à l'ordinateur. Si le nombre est correct, l'utilisateur aura accès au système.

Exemple : . transformation logique :

L'ordinateur envoie un mot de passe de cinq chiffres.
L'utilisateur y additionne la date du jour et renvoie, par exemple, une paire de chiffres du résultat.

. transformation mathématique :

L'utilisateur sait que son mot de passe est la fonction algébrique suivante :

$$2x + z^2$$

La procédure d'identification sera la suivante :

```
+TYPE YOUR SECURITY CODE
/I26
+IF X=5, Z=2, WATH IS THE PASSWORD?
/I4
+PROCEED
```

Dans ce dernier exemple, la complexité de la fonction algébrique dépendra éventuellement du niveau de sécurité requis et du niveau de formation des utilisateurs des terminaux.

5.2.I.7. IMPLEMENTATION.

La procédure d'identification est basée sur l'utilisation d'une "table des mots de passe" stockée sur un fichier permanent (voir Fig. 5.2.I.7.) :

- chaque entrée de la table associe un mot de passe à un utilisateur. (la procédure d'identification se terminera normalement si l'utilisateur introduit le mot de passe associé à son nom).
- Le fichier contenant la table des mots de passe :
  - . est accessible à la procédure d'identification (consultation) et à une seule personne (maintenance): le responsable de la sécurité du système.
  - . n'est accessible à aucun utilisateur, tant en consultation qu'en mise à jour.
- L'intégrité du système dépend donc de l'aptitude à garder la table secrète.

5.2.I.8. INCONVENIENT DE LA PROTECTION PAR MOT DE PASSE.

. Le responsable de la sécurité du système connaît les mots de passe des utilisateurs ou peut les connaître en demandant l'impression de la totalité ou d'une entrée de la table or,

a) il n'y a aucune raison qu'il les connaisse (les mots de passe pourraient être générés automatiquement) ;

b) un listing de la table obtenu par le responsable, dans un but de contrôle, peut toujours être vu par inadvertance par une personne non-autorisée. Remarquons que même des listings périmés pourraient apporter des informations (structure des mots de passe) à un utilisateur non-autorisé. (Notons qu'il existe des machines réduisant les documents confidentiels (listings) en copaux ou confettis en quelques instants.)

. Toute personne accédant à la salle machine (sécurité physique) peut commander une impression de la table à partir de la console (sans passer par les fonctions d'identification et d'autorisation).

;. Un dispositif de protection basé sur l'utilisation de mots de passe ne pourra donc être implémenté si le système de sécurité des données n'offre pas la possibilité de protéger les fichiers contre une lecture non-autorisée.

Nous décrirons ci-après une procédure qui, moyennant certaines hypothèses, permet de démontrer comment pallier à ces inconvénients.

5.2.I.9. AMELIORATION DE LA TECHNIQUE DE PROTECTION PAR MOT DE PASSE.

A. SUPPRESSION AUTOMATIQUE DE L'IMPRESSION/VISUALISATION.

Il est utile d'empêcher la visualisation ou l'impression d'un mot de passe lorsqu'il est introduit, afin de diminuer le risque qu'il soit observé par une autre personne.

Les techniques suivantes sont le plus souvent utilisées :

. INHIBITION AUTOMATIQUE :

Sur certains terminaux, l'ordinateur peut demander un mot de passe et empêcher conjointement son impression ou sa visualisation sur le terminal.
L'inhibition automatique réalisée par l'ordinateur (utilisation de lignes de transmission en full-duplex) est une opération plus discrète que la procédure où l'utilisateur introduit son code, d'une main, tout en appuyant sur une touche du clavier (télétype) ou en baissant, de l'autre main, l'intensité lumineuse (terminal à écran)

. SURIMPRESSION DE CARACTERES QUELCONQUES

Si le code de sécurité est, par exemple, de 6 digits, l'ordinateur envoie une série de caractères quelconques qui noircissent un emplacement nécessaire à 6 digits, (par un va-et-vient du dispositif d'impression).

La tête d'écriture se repositionne ensuite au début de la zone et l'utilisateur introduit son code de sécurité.

Exemple : +TYPE YOUR PASSWORD
/######
+ USER NAME
/426,SMITH
+PROCEED
/ - transaction -

B. FONCTION D'IDENTIFICATION NE NECESSITANT AUCUNE PROTECTION DE LA TABLE DES MOTS DE PASSE.

I. HYPOTHESE : Une personne non-autorisée ne sera jamais capable d'accéder au système, même si tous les éléments de la procédure d'identification (sauf les mots de passe) lui sont accessibles.

2. PRINCIPE DE FONCTIONNEMENT : (voir Fig. 5.2.I.9 a)

PHASE I : L'utilisateur voulant accéder au système introduit : . son numéro d'identification ou son nom;
. un mot de passe.P.

PHASE 2.: Une procédure détermine la valeur d'une fonction H au point P.
Remarque : H est un programme dont l'unique paramètre d'entrée est P, c'est-à-dire le mot DE PASSE (de n bits) entré par l'utilisateur. Il consiste à générer n bits à partir des n bits de P. (Le résultat obtenu est en fait un cryptogramme - voir section 7).

PHASE 3 : Le résultat obtenu , soit H(P), est comparé à la clé résidant dans l'entrée correspondant à l'utilisateur dans une table des clés (table identique à la table des mots de passe décrite précédemment).
Si E=H(P), l'utilisateur est accepté du fait qu'il connaît une valeur de P qui permet de produire une valeur tabulée E. (la mise à jour de la table des clés peut se faire indépendamment du responsable de la sécurité :
Exemple : en fin de session terminal, l'utilisateur peut au moyen d'une commande spéciale, envoyer un mot de passe qui générera une nouvell clé ainsi qu'une mise à jour de l'entrée correspondante de la table).

Remarque : On suppose que toute personne non-autorisée, voulant accéder au système, sera susceptible d'accéder à la fonction H (lecture du programme) et à la table des clés. (voir hypothèse de départ).

Etant donné que l'intégrité du système se trouvera menacée si cette personne arrive à déduire l'entrée (P) à partir d'un résultat (E) de la table, il est nécessaire d'avoir une fonction H très difficile à inverser.
Dans ce but, on va baser la procédure d'identification sur :

- l'utilisation d'une famille de fonctions (H) de transformation d'un P en E.
- le choix de H, dans la famille en fonction du mot de passe introduit ; en résumé :
  - pour un mot de passe P donné, on considère une fonction F_P (dont le choix dépend de P lui-même) parmi la famille qu'on s'est donnée.
  - la valeur E, dans la table des clés, sera F_P (P).

En tenant compte de la rapidité de calcul des processeurs actuels, on peut répéter plusieurs fois le processus de sélection de la fonction F_P afin d'accroître la complexité de la procédure.

3. DESCRIPTION DE LA PROCEDURE. (voir Fig. 5.2.I.9 b et c).

Le calcul que la fonction H doit réaliser, comporte J cycles (3) :

- chaque cycle convertit (7) un mot de passe (ou ensemble de bits) en un autre. (Nous appellerons "clé" le dernier obtenu, c'est-à-dire celui figurant dans la table) ;
  - ° cycle I : utilise le mot de passe P introduit par l'utilisateur (2) ;
  - ° cycle 2 à J : utilise l'ensemble de bits fourni par le cycle qui le précède (7). (voir Fig. 5.2.I.9. b)
- chaque cycle est paramétré par une valeur différente (du point de vue traitement, chaque cycle est donc distinct) :
  - ° cycle I : est paramétré par P (I) ;
  - ° cycle 2 à J : le paramètre est déterminé en appliquant la fonction Next X (n bits) au paramètre du cycle précédent (8).

(La fonction calculée par un cycle est appelée F_X (le paramètre X est de la même forme que P et est généré au hasard, par exemple).

- chaque cycle consiste à appliquer successivement et dans un ordre déterminé, K fonctions (f_1, f_2, ... f_K) de transformation d'un ensemble de bits (mot de passe actuel) en un autre (4).

  ° Chaque fonction f_K :

  . est paramétrée par X (le paramètre du cycle) et/ou par P (mot de passe introduit par l'utilisateur) ;

  . est répétée m fois (6) (m dépend de la valeur actuelle de X et de P. (5)).

En résumé : La boucle intérieure (6) représente les m répétitions d'une même fonction de transformation f_K (7).

La boucle intermédiaire (4) consiste à appliquer K fonction f_K (5) (6) tandis que la boucle extérieure représente les J cycles (4) (8).

4. EFFICIENCE DE LA PROCEDURE.

Il est intéressant d'examiner brièvement les difficultés qui surgissent en cas de tentatives de violation de procédure.

Considérons, par exemple, les événements suivants :

- soit E, la clé correspondant à l'utilisateur dans la table des clés;
- soit g, la dernière fonction f_K utilisée ;
- soit Q, la valeur à laquelle g fut initialement (avant les m boucles) appliquée,
- soit m, le nombre de fois que g a été exécuté.

On a donc : $E = g^m (Q)$

D'après l'hypothèse de départ, une personne non autorisée voulant accéder au système, pourrait connaître E, g et même g^{-1}

Nous constatons qu'il lui est impossible de retrouver le mot de passe P correspondant à une clé E; en effet :

- la connaissance de E, g et g^{-1} ne lui sera d'aucune utilité puisqu'il ne connaît pas m, (or, m dépend de P)
- plusieurs applications de g^{-1} à E et l'examen du résultat obtenu après chacune de celles-ci ne lui sera d'aucune utilité puisque rien ne lui permettra de reconnaître Q lorsqu'il l'obtiendra.

En pratique, la difficulté d'inverser H sera proportionnelle :

- au nombre de fonctions f_K utilisées,
- au nombre de cycles parcourus,
- à la longueur (nombre de bits) du mot de passe P,
- à la difficulté d'inverser les fonctions f_K.

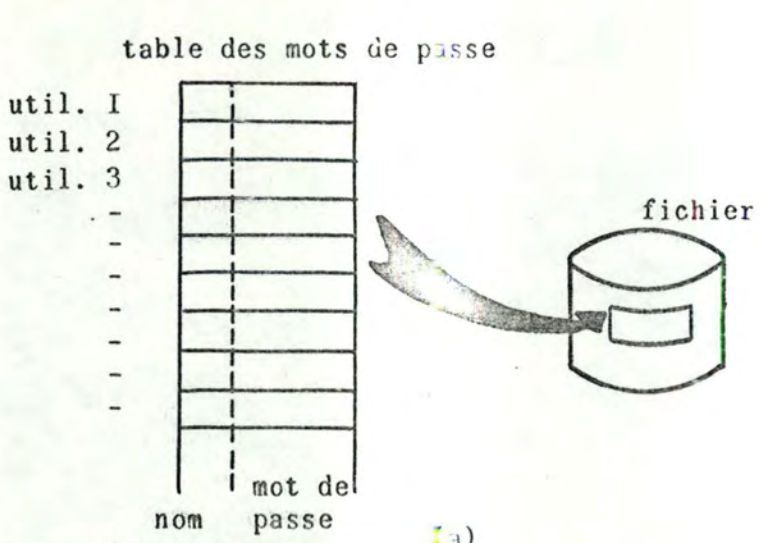
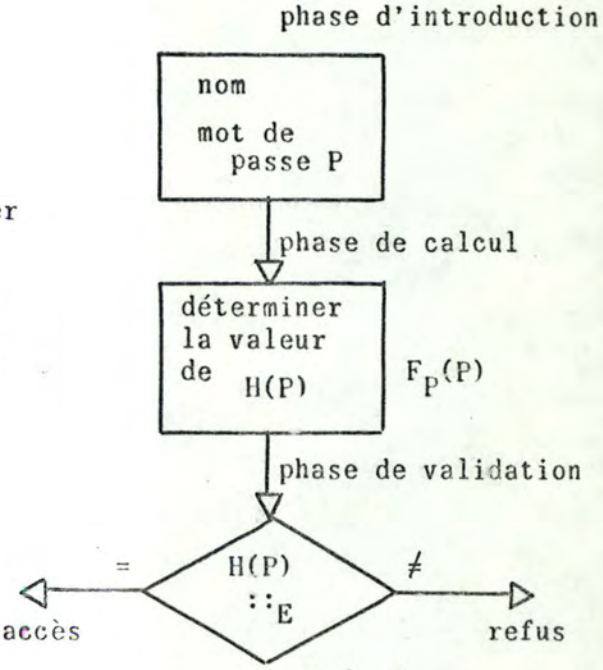
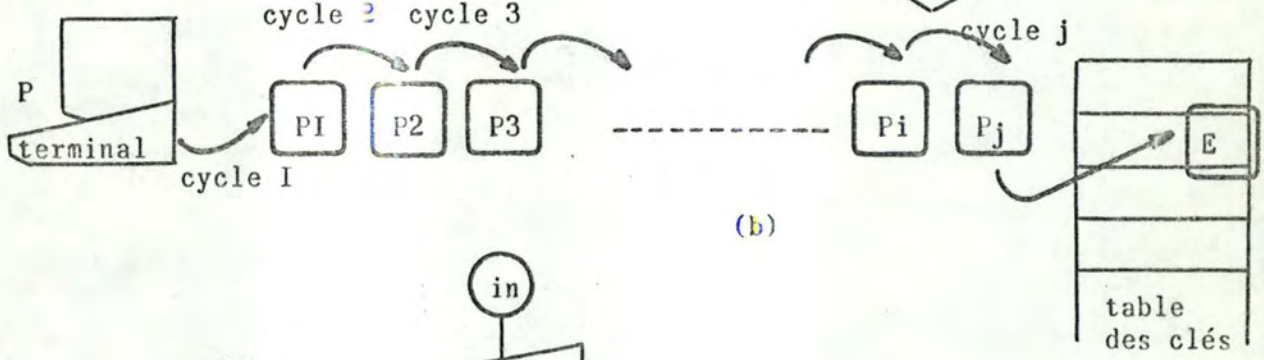


fig. 5.2.I.7

(a)



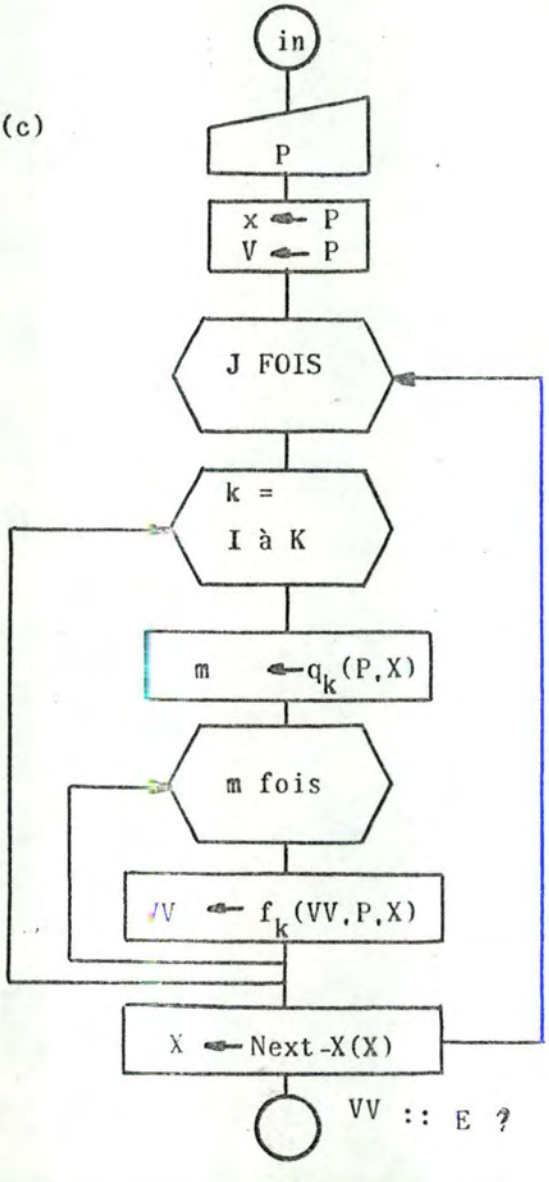
(a)



(b)

(c)

Fig. 5.2.I.9



Remarque : Vu la difficulté d'obtenir un P correspondant à une clé E connue, nous admettrons qu'il puisse éventuellement exister des mots de passe distincts (soit P_1, P_2) qui conduisent à la même clé.

5. EXEMPLE :

- Système de protection par mots de passe utilisés dans MULTICS. (voir références en bibliographie).

5.2.2. SEQUENCE DE QUESTIONS REPONSES.

5.2.2.I. PRINCIPE.

L'ordinateur pose à l'utilisateur une série de questions personnelle choisies au hasard parmi plusieurs précédemment stockées dans le système; les questions sont choisies de telle façon que lui seul est capable d'en donner la réponse correcte. Elles se rapportent toujours à des informations personnelles. Il ne risque donc pas d'en oublier la réponse comme c'est le cas, lors de l'emploi de mots de passe ou de sécurité.

5.2.2.2. FONCTIONNEMENT.

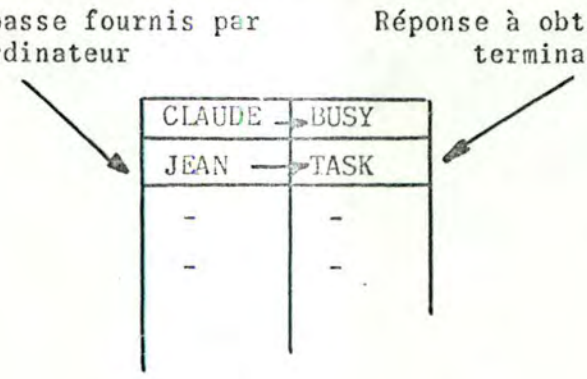
Un ensemble de questionsainsi que les réponses correspondantes ont été mémorisées lors de la génération du système d'identification.
L'ordinateur peut poser d'autres questions à chaque session terminal; il peut aussi varier leur ordre, ce qui exclut la possibilité, pour une autre personne, d'observer les réponses à toutes les questions.
Note : L'impression des réponses sera de préférence inhibée automatiquement par l'ordinateur.

Exemples de questions-réponses :

. QUESTIONS PERSONNELLES :

Quelle est la date de naissance de votre femme, celle de votre mariage ou le nom de votre grand-mère.?.

. TABLES DES MOTS DE PASSE ET DE LEURS REPONSES PRECISES:



5.2.2.3. CRITIQUE DU SYSTEME

Avantages : facilité d'utilisation ; haut degré de sécurité lorsque ce système est utilisé en conjonction avec des mots de passe ou badges.

Inconvénients : / durée de la procédure d'identification,
. degré de sécurité peu élevé :
- si les questions sont trop simples;
- si elles sont identiques pour tous les utilisateurs ;
- si les réponses peuvent être facilement trouvées (ex. : dans le fichier du personnel, date de naissance de l'utilisateur; n° de téléphone etc...)

. l'efficacité du système est inversément proportionnelle à la durée de la période comprise entre deux renouvellements des questions, (c'est-à-dire à la fréquence d'utilisation de la procédure).
. place mémoire (tables ou questions-réponses).

5.3. IDENTIFICATION PAR UN OBJET QUE LA PERSONNE PEUT GARDER SUR ELLE.

5.3.I. PRINCIPE

Une autre procédure qui utilise avec succès la mémorisation de nombres consiste à encoder optiquement ou magnétiquement des informations pour identifier l'utilisateur du terminal.
Remarquons que les cartes ou badges encodés optiquement sont moins sûrs que celles encodées magnétiquement car le codage y apparaît clairement.

5.3.2. FONCTIONNEMENT

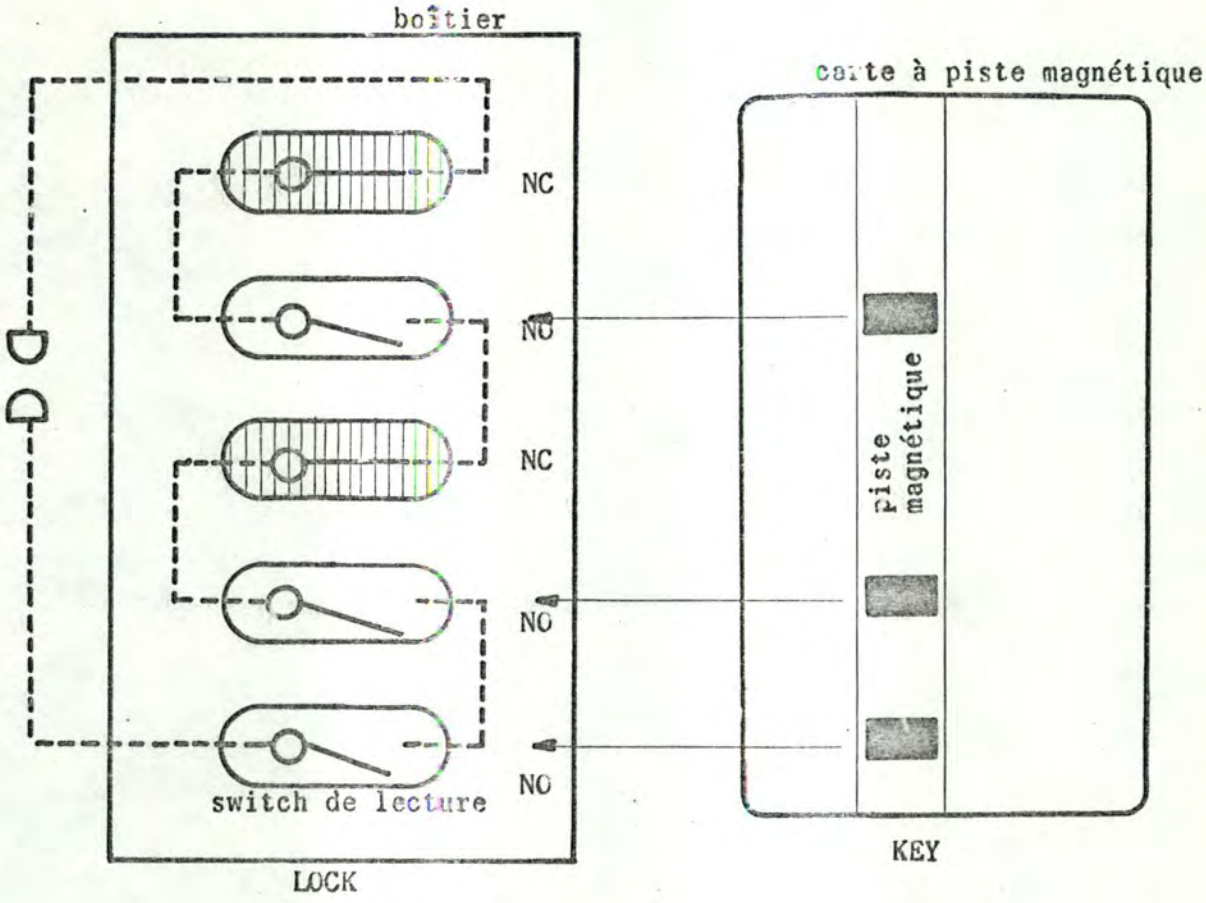
La procédure d'identification peut être réalisée de plusieurs manières. L'adoption d'une procédure plutôt que d'une autre dépend du degré de sécurité qu'on désire obtenir. L'introduction de la carte dans le lecteur sera suivie soit :

I. du test de validité du code de sécurité enregistré sur la carte (application d'une procédure de calcul sur la clé)
ex. : addition, soustraction, multiplication ou division d'une/par une quantité, transformations sur les caractères.

2. de la comparaison de la clé de la carte avec une clé mémorisée.

3. de l'introduction d'un code au clavier, transformation de ce code et comparaison au code de la carte.

La figure 5.3.2. décrit un bloc de lecture. Dans cet exemple, tous les utilisateurs autorisés à se servir du terminal ont le même badge. La présence d'un strip magnétique sur le badge entraîne la fermeture du switch correspondant dans le bloc de lecture. L'efficacité du dispositif est proportionnelle au nombre de switchs.



5.3.3. AVANTAGES DE LA PISTE MAGNETIQUE.

I. Difficulté de reproduction (en cas de vol) :

Une carte à piste magnétique ne peut être aussi facilement reproduite qu'une clé.
Exemple : Que peut-il se passer si une personne non-autorisée entre en possession du badge d'un utilisateur ?

- Il lui serait possible de lire l'information de la piste magnétique (il existe des loupes prévues à cet effet) et donc de connaître le numéro de code de l'individu à qui il a dérobé le badge.
- Le danger n'apparaît ici que dans la mesure où il lui est possible de reproduire le code de sécurité.

2. Simplicité de la procédure d'identification.

5.3.4. INCONVENIENTS ET AMELIORATIONS DU SYSTEME.

I. Perte ou vol.

Les clés, badges et cartes de crédit ont en commun cet inconvénient : elles peuvent être perdues ou dérobées.

- AMELIORATIONS : Annulation de la carte sur ordre de l'utilisateur.

De préférence, la carte ne comportera aucune inscription visible; en cas de perte, l'utilisateur préviendra directement le responsable de la sécurité. Ce dernier invalidera la carte perdue en modifiant la table des mots de passe ou codes sécurité du programme d'identification.

Annulation imprévue et revalidation.

Régulièrement (tous les mois) ou de façon imprévue, le responsable d'un département peut récupérer les badges des utilisateurs. Avant de les revalider (modification du mot de passe) une simple lecture de chacune d'entre elles fera apparaître les duplications éventuelles.

Détection d'un emprunt.

Si la piste magnétique contient plusieurs mots de passe utilisables une seule fois (voir 5.2.I.6.2), et si le dispositif de lecture remet à blancs le dernier mot de passe utilisé, l'utilisateur peut détecter tout emprunt de sa carte. Connaissant le nombre de mots de passe qu'il peut encore utiliser, il s'apercevra de l'utilisation de l'un de ceux-ci (vu la remise à blancs) dès la première session terminal.

2. Négligence de l'utilisateur.

Ex : - oubli de la carte dans le lecteur ;

- AMELIORATION : Prévoir un autre lecteur à la sortie de la pièce où se trouve le terminal.

5.3.5. REMARQUE -
Un badge ou une carte à piste magnétique seront particulièrement efficaces s'ils sont combinés à un système d'alarme en cas d'effractions, ou utilisés en conjonction avec un code de sécurité introduit au clavier. Carte et code sont alors tous deux nécessaires pour avoir accès au système.

5.4. IDENTIFICATION AU MOYEN DE CARACTERISTIQUES PERSONNELLES.

Il existe de nombreuses caractéristiques physiques qui permettent de reconnaître une personne, si pas avec certitude, du moins avec une très faible probabilité d'erreur.

Plusieurs brevets ont été obtenus pour des dispositifs qui voulaient enregistrer une mensuration identifiable de l'individu. Certains de ceux-ci sont très coûteux; par exemple, les lecteurs d'empreintes digitales ou les dispositifs à entrée vocale commercialisés depuis peu. D'autres sont peu réalistes ; détecteurs d'odeurs, lecteurs d'empreintes des lèvres, dispositifs pour mesurer la forme de la tête, etc...

5.4.I. DISPOSITIF D'ENREGISTREMENT DE LA VOIX.

5.4.I.I. PRINCIPE :

L'utilisateur prononce une phrase déterminée à l'avance, par exemple, les chiffres d'un numéro de code, et un dispositif à l'entrée de l'ordinateur convertit les sons en un ensemble de bits. Le système compare ensuite cet ensemble de bits à un autre ensemble mémorisé précédemment et provenant lui aussi des mêmes sons prononcés par l'utilisateur.

Comme les voix des utilisateurs diffèrent quelque peu de temps à autre (nervosité, fatigue, émotion...); le système ne retient que certains paramètres caractéristiques et ne compare que ceux-ci en examinant s'ils se situent à l'intérieur des limites admissibles de variation.
L'analyse de la voix humaine est complexe et est encore une technologie en cours de développement : comme le débit de la voix peut varier constamment, il faut d'abord une synchronisation de ce débit avec celui du modèle qui fera l'objet de la comparaison; après cette synchronisation, la variation de ton (vitesse de vibration des cordes vocales) et d'intensité (son) peut être comparée avec le modèle.
Bien d'autres caractéristiques peuvent encore être prises en considération.

5.4.I.2. DEFAILLANCES ET CRITIQUE DU SYSTEME.

L'imitation de la voix de l'utilisateur par un imposteur va augmenter considérablement le taux d'acceptations illégales. Elle présente néanmoins beaucoup de difficultés pour avoir une efficacité suffisante (ex. : utilisation d'un enregistrement sur bande magnétique du texte d'identification prononcé par la personne).

La principale difficulté dans les systèmes de reconnaissance de voix réside dans le fait qu'il n'est presque pas possible de reconnaître une personne enrhumée ou étant sous la menace; si on augmente les limites admissibles de variation des différents paramètres de la voix pour accepter ces cas particuliers, la probabilité d'une acceptation illégale va augmenter considérablement.

Remarquons qu'il serait possible de digitaliser la voix humaine dès le terminal et non à l'arrivée à l'ordinateur. Nous aurions un train de bits sur la ligne de transmission, mais l'utilisateur perdrait l'avantage de n'avoir besoin d'aucun équipement supplémentaire pour l'identification, si ce n'est que d'un téléphone ordinaire.

5.4.I.3. EXEMPLE : UNITE A ENTREE VOCALE VIP 100 MISE AU POINT PAR LA SOCIETE THRESHOLD TECHNOLOGY.

Un VIP 100 de 8 K peut "comprendre" 32 mots de vocabulaire, le "mot" étant défini comme une courte phrase de moins de 25 secondes. Lorsque plusieurs opérateurs (3 au maximum) se servent d'une même unité, chacun possède son propre vocabulaire et son code d'identification qu'il annonce lorsqu'il initialise une session terminal. Le temps de réponse (décodage de la voix) est inférieur à un dixième de seconde, le temps minimum entre deux mots est de deux dixièmes de seconde.

5.4.I.4. CONCLUSIONS.

L'opération de reconnaissance de la voix ne suffit pas pour identifier infailliblement l'utilisateur. Utilisée conjointement avec un autre moyen d'identification, tel qu'un numéro secret, elle pourra procurer un haut degré de sécurité.

5.4.2. DISPOSITIF BASE SUR LA GEOMETRIE DE LA MAIN

Il est très rare que deux personnes aient la même forme de main, si bien que ses caractéristiques peuvent fournir un meilleur moyen de reconnaissance individuelle que l'enregistrement de la voix. Un des premiers appareils capables d'assurer l'identification automatique d'une personne par un dispositif basé sur la lecture de caractéristiques des mains vient d'être commercialisé sous le nom d'IDENTIMAT 2000.

5.4.2.I. PRINCIPE :

Des études statistiques ont démontré qu'il n'existe pratiquement pas deux mains présentant une géométrie identique. Utilisant cette donnée, l'appareil enregistre fidèlement sur une carte d'identification à piste magnétique, les mensurations de la main pour ensuite les lire et les comparer à la main du porteur de la carte. (voir Fig. 5.4.2.I)
On écarte ainsi toute possibilité de fraude par prêt, vol ou perte de carte. Seul, le titulaire peut être utilisable sans carte.

5.4.2.2. FONCTIONNEMENT :

Les données relatives à la géométrie de la main de l'utilisateur et celles caractérisant les locaux auxquels il a accès, sont codées magnétiquement sur la carte, en une seule opération.(voir Fig. 5.4.2.2.)
Pour obtenir l'autorisation d'entrer , l'utilisateur introduit verticalement sa carte dans une fente sur la face supérieure de l'appareil et place sa main à plat, sur le dispositif de lecture, dans la position imposée par le guide. L'IDENTIMAT 2000 compare alors automatiquement la géométrie de cette main avec les mensurations codées sur la carte magnétique et émet un ordre "Accepté" ou "Refusé" qui permet l'ouverture d'un accès (porte,...) ou la transmission du numéro d'identification de l'utilisateur ainsi que celui de l'appareil utilisé.

5.4.2.3. CRITIQUE DU SYSTEME :

Le dispositif prend I2 mesures dont notamment la longueur des doigts : une analyse des longueurs des doigts d'environ 4000 personnes a montré que si on utilise la longueur des quatre doigts d'une même main pour identifier une personne, la probabilité de reconnaissance erronée est par exemple de 0,5 % si les tolérances de mesure sont sont ± I.5 mm. La probabilité de rejeter une personne, alors qu'elle peut avoir accès au système, est très faible.

L'IDENTIMAT 2000 utilise une lumière intense qui rend translucide les extrémités des doigts. Il mesure dès lors la transmission de la lumière à travers ces extrémités de doigts, ce qui empêche une personne avec de longs ongles, d'être rejetée et rend très difficile d'induire en erreur le dispositif en portant sur soi un gant fait soigneusement aux mesures d'une autre personne.

5.4.2.4. EXEMPLE D'UTILISATION :

Identification d'utilisateurs de cartes de type badge, (voir Fig. 5.4.2.4.) pour l'accès aux programmes et fichiers.

5.4.2.5. REMARQUES :

Durée du codage d'une carte : moins de 2 minutes.
(mensuration de la main, numéro d'identification de l'employé, locaux dont l'accès lui est permis, numérotation de la carte, privilèges éventuels...)

Durée du cycle de comparaison entre la géométrie de la main placée sur l'appareil et les données codées sur la carte d'identification: moins d'une seconde.
(mesure de la main, lecture de la carte et vérification de l'identité

5.4.3. IDENTIFICATION ET VERIFICATION : DEGRE D'EFFICACITE.

5.4.3.1. COUT DE L'OPERATION DE VERIFICATION.

On constate, dans tous les dispositifs de reconnaissance des caractéristiques physiques d'une personne, une disproportion entre l'identification d'un individu et la vérification que cet individu est bien ce qu'il prétend être.
Dans les systèmes de reconnaissance d'empreintes digitales ou d'enregistrements de la voix, l'identification a été plus largement développée que la vérification.
Celle-ci est cependant beaucoup moins coûteuse, l'ordinateur n'ayant qu'à prendre une décision binaire ;

- OUI, l'utilisateur est bien ce qu'il prétend être,
- NON, ce n'est pas cette personne.

Exemple : En comparant l'empreinte du pouce d'une personne avec une empreinte préenregistrée, par exemple, une simple comparaison optique peut être faite au centre de l'empreinte digitale où la distorsion est moindre.
Ceci est, de loin, moins coûteux que d'essayer d'analyser l'entièreté des empreintes.

5.4.3.2. MESURES DE L'EFFICACITE.

Un dispositif de vérification peut commettre deux types d'erreurs :

- un rejet erroné (la personne est bien ce qu'elle prétend être mais le dispositif la rejette;)
- une acceptation illégale (le dispositif accepte une personne alors qu'il devrait la rejeter.)

Il faut donc considérer deux mesures de l'efficacité d'un dispositif :

1. la probabilité de rejets erronés,
2. la probabilité d'acceptations illégales.

Dans ces dispositifs, une diminution de la probabilité d'acceptations illégales tend à accroître la probabilité de rejets erronés.

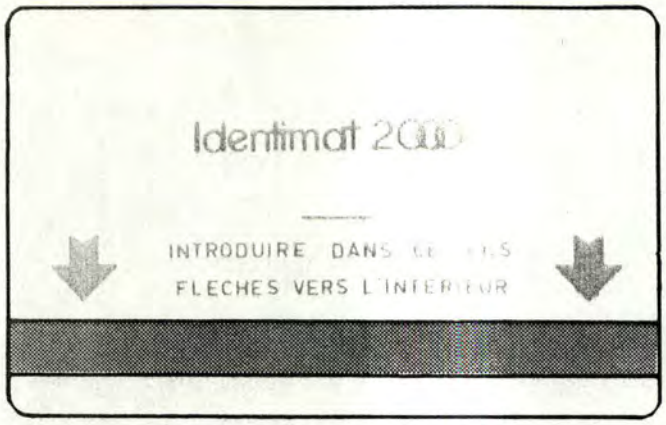


fig. 5.4.2.2

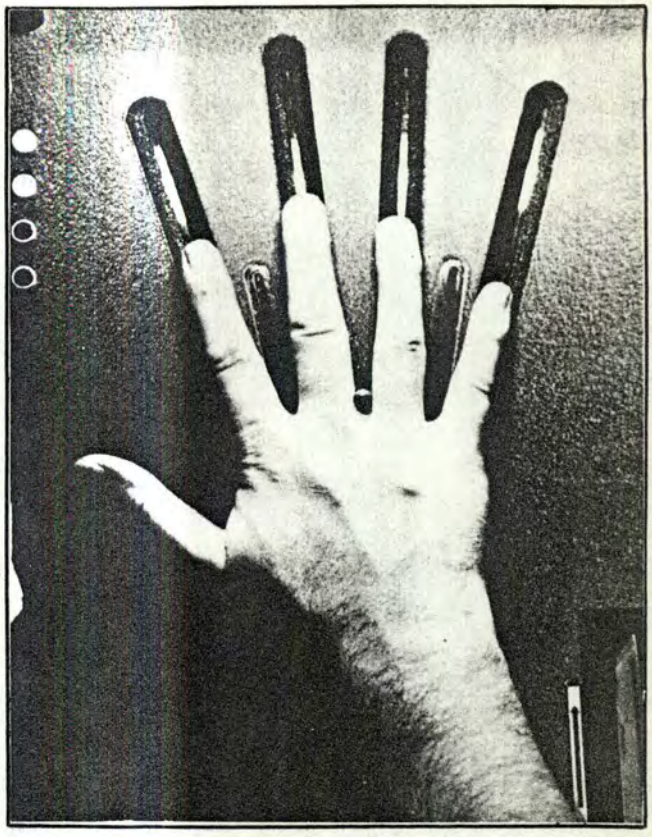
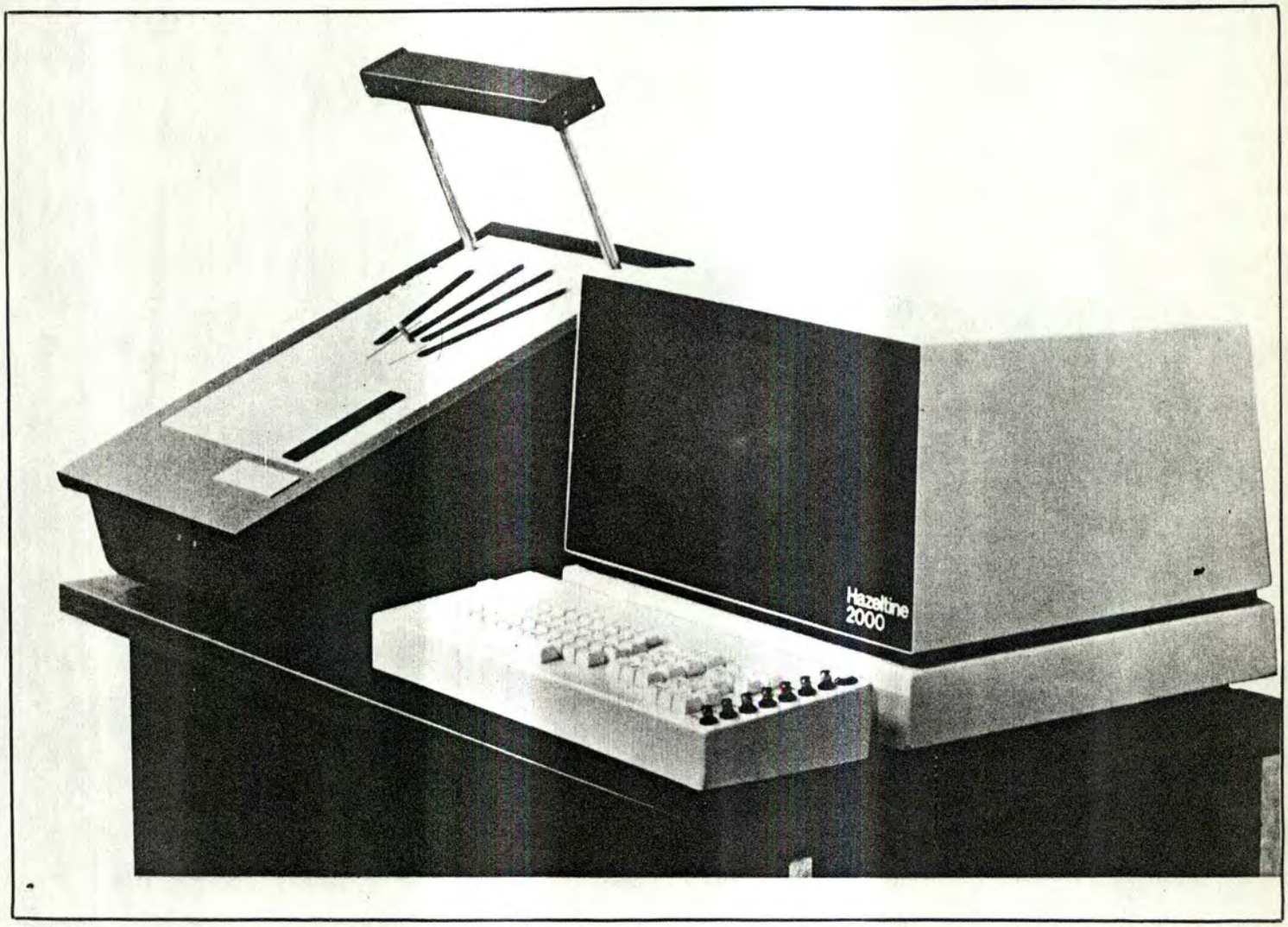


fig. 5.4.2.I

fig. 5.4.2.4



5.5. CONCLUSIONS.

Si les ressources (programmes et données) d'un système de télétraitement n'ont aucune valeur ou ne sont d'aucun intérêt pour les personnes autres que leur propriétaire, il ne sera pas nécessaire de mettre en place un système hardware ou/et software d'identification.

Toutefois, si ces ressources contiennent des informations de niveaux de confidentialité différents suivant les utilisateurs, la conception et la mise en place d'un système d'identification permettra de sauvegarder la sécurité et l'intégrité de celles-ci. Graduellement, un système d'identifications pourrait être étendu de façon à couvrir les fonctions d'identification mentionnées à la Fig. 5.5.

Remarque :
La recherche de dispositifs assurant une plus grande sécurité risque :

- d'allonger la durée de la procédure d'identification,
- de consommer une place mémoire de plus en plus importante (programme d'identification, tables de mots de passe).

Une dernière remarque à formuler : quelle que soit l'approche choisie pour identifier l'utilisateur, le programme d'identification ainsi que les tables de mots de passe nécessitent une protection supplémentaire. Dans la plupart des cas, ces tables font partie intégrante du système d'exploitation. Toute modification de celles-ci ne pourra se faire sans l'obtention d'un mot de passe spécial réservé au responsable de la sécurité du réseau de communication et des données.

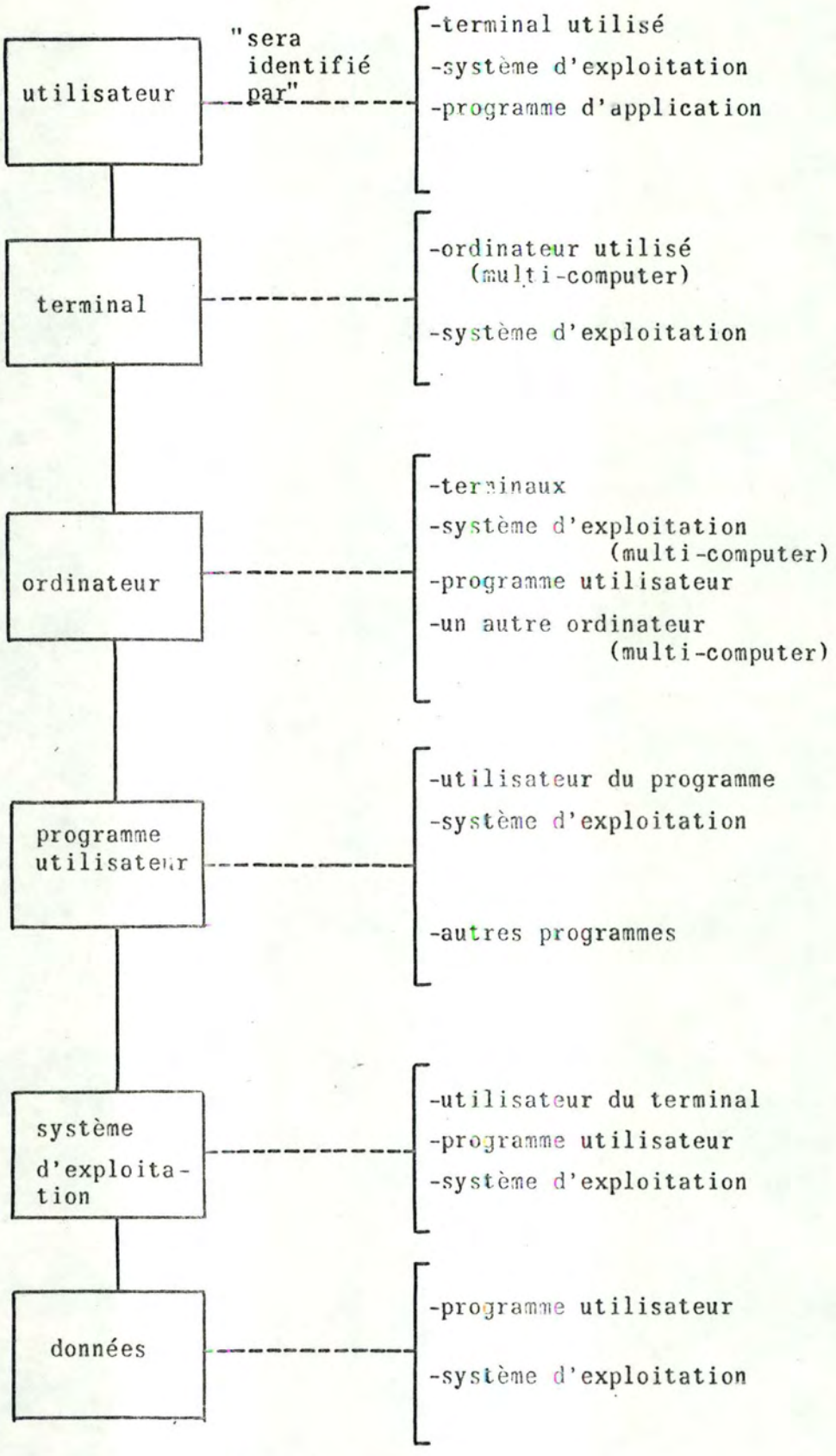

utilisateur
"sera identifié par"
-terminal utilisé
-système d'exploitation
-programme d'application
terminal
-ordinateur utilisé (multi-computer)
-système d'exploitation
ordinateur
-terminaux
-système d'exploitation (multi-computer)
-programme utilisateur
-un autre ordinateur (multi-computer)
programme utilisateur
-utilisateur du programme
-système d'exploitation
-autres programmes
système d'exploitation
-utilisateur du terminal
-programme utilisateur
-système d'exploitation
données
-programme utilisateur
-système d'exploitation

fig. 5.5

section 6 : fonction d'autorisation d'accès.

6.I. RAPPEL.

Les procédures de contrôle d'accès au terminaux et d'identification du terminal utilisé ou de l'utilisateur de celui-ci nous ont obligé à scinder l'ensemble des utilisateurs en 3 catégories (voir Fig. 6.I a).

Chaque utilisateur a donc :

- soit accès à tous les terminaux - protégés ou non (I) ;
- soit accès aux terminaux non protégés seulement (2)
- ou accès à aucun de ceux-ci. (3)

Pour chaque catégorie d'utilisateurs, la Fig. 6. I b donne les types de protection qui peuvent être envisagés.

En pratique,

- le choix de la répartition à adopter dépendra de plusieurs facteurs tels que :
  - . l'organisation du service informatique, le partage des responsabilités, la confiance au personnel...
  - . l'importance des données à traiter (confidentielles ou non) ainsi que des programmes,
  - . le nombre de terminaux.
- le choix et la mise en place de dispositifs de protection hardware ou software (procédure d'identification) résultera :
  - . d'une analyse d'opportunité préalable,
  - . du degré de sécurité à assurer.

6.2. ROLE DE LA FONCTION D'AUTORISATION.

La fonction d'identification nous a permis de déterminer les utilisateurs autorisés à accéder au système; la phase suivante (voir Fig. 6.2. établira le niveau ou le degré d'autorisation de chacun d'eux et sera réalisée par la fonction d'autorisation.

6.3. IMPORTANCE DU DEGRE D'AUTORISATION.

L'établissement d'un degré d'autorisation consiste à accorder un ensemble de privilèges à chaque utilisateur.
Un privilège consiste, par exemple, en une autorisation de lire, d'écrire, ou de modifier certains enregistrements ou items ou encore d'utiliser certains programmes d'application ou utilitaires.

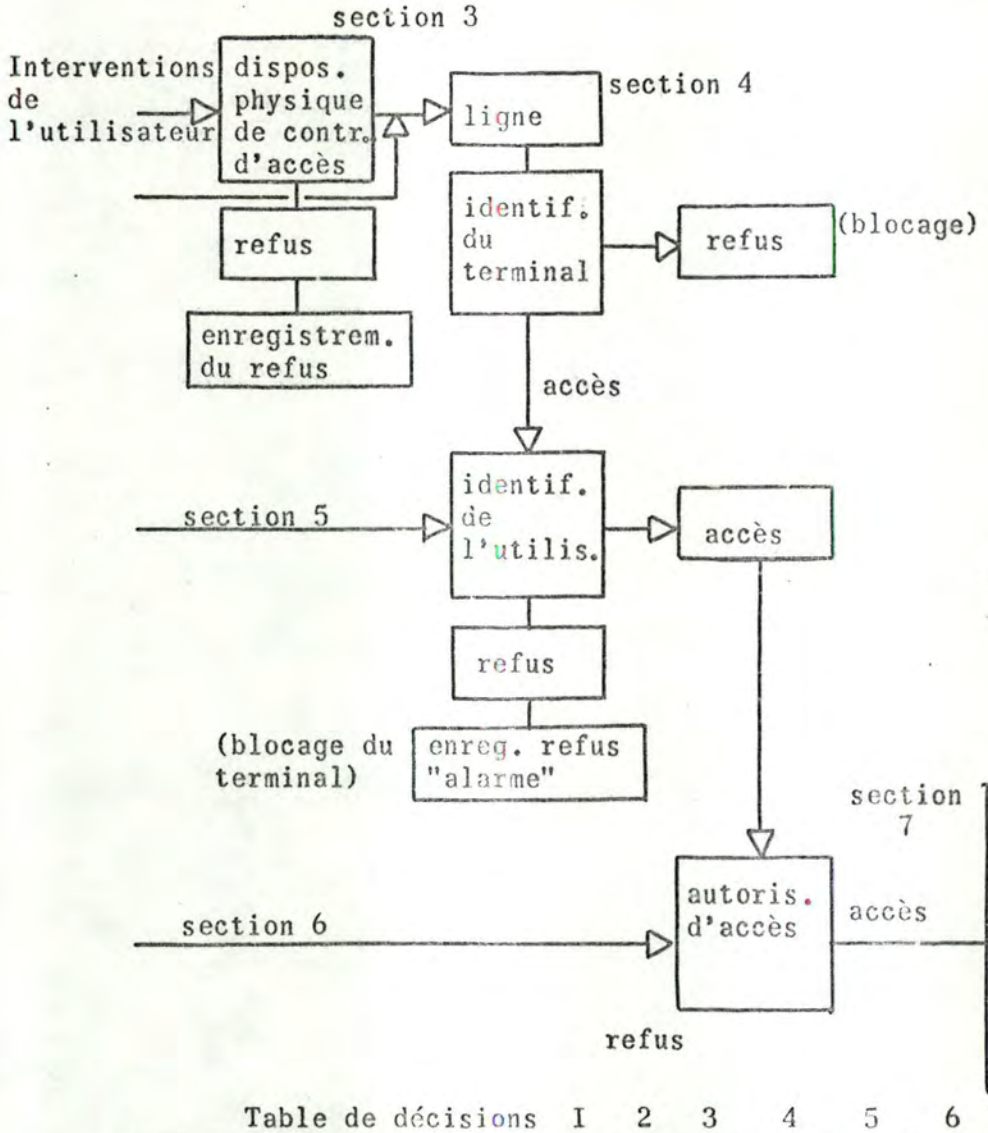


fig. 6.I a)

Table de décisions I 2 3 4 5 6

catégories d'utilisat.						
(I) accès à tous les T.	x			x	x	
(2) accès aux TNP		x		x		x
(3) accès à aucun T			x		x	x
☐ dispositif de protection/ local				x	x	x
☐ protection sur le terminal				x	x	x
☐ identification du terminal	x	x		x	x	x
☐ identification de l'utilisateur	x	●		x	x	●

T: terminaux
TNP: term. non protégés

●: facultatif

○: "ou"

section 3

section 5

fig. 6.I b)

Le concept de degré d'autorisation doit être nécessairement introduit lorsque la base de données accessibles à plusieurs utilisateurs, contient des informations de niveaux de confidentialité différents.

Exemple : L'utilisateur pourra : (voir fig. 6.2)

- au niveau de la base de données : lire certains fichiers, (le terme fichier désigne une partie de la base de données ou ensemble des enregistrements d'un même type sans pouvoir les modifier,
- au niveau d'un fichier de la base : introduire des données, sans pouvoir lire le contenu du fichier,
- au niveau d'un enregistrement : lire, écrire et/ou modifier certains items de l'ensemble ou d'une partie des enregistrements d'un même type.

  De plus, un statisticien peut être amené à travailler sur l'ensemble des enregistrements "PERSONNE" d'un fichier "PERSONNEL" il doit dans ce cas :

  - pouvoir obtenir l'étendue des valeurs de l'item "traitement mensuel" ou encore l'ensemble des noms des membres du personnel. (I)
    Toutefois, il ne pourra pas réaliser l'établissement d'une corrélation entre les items "Nom" et les items "Traitement". (2)

    Conséquence de(I) : les items "Nom" et "Traitement" doivent pouvoir être accessibles lors d'un opération de lecture (consultation).

    Conséquence de(2) : comme les items "Nom" et "Traitement" font partie d'un même enregistrement, ils ne peuvent être fournis simultanément en réponse à une opération de consultation.

Les problèmes provenant de l'utilisation de bases de données à des fins statistiques devront être traités plus rigoureusement.

De même que la base de données, qu'un fichier, qu'un enregistrement ou qu'un item, un programme peut être partagé entre plusieurs utilisateurs. Remarquons que l'utilisation d'un programme peut entraîner son altération et donc l'obtention d'informations non-autorisées s'il n'y a pas de protection au niveau des fichiers.

Lorsque des violations de la sécurité se produisent, le software doit pouvoir automatiquement :

- verrouiller le terminal (interruption de la communication et/ou "abend" du programme),
- enregistrer et analyser la tentative de violation (heure et type de transaction, terminal, n° d'identification de l'utilisateur.., objet de la tentative),
- avertir éventuellement le responsable de la sécurité.

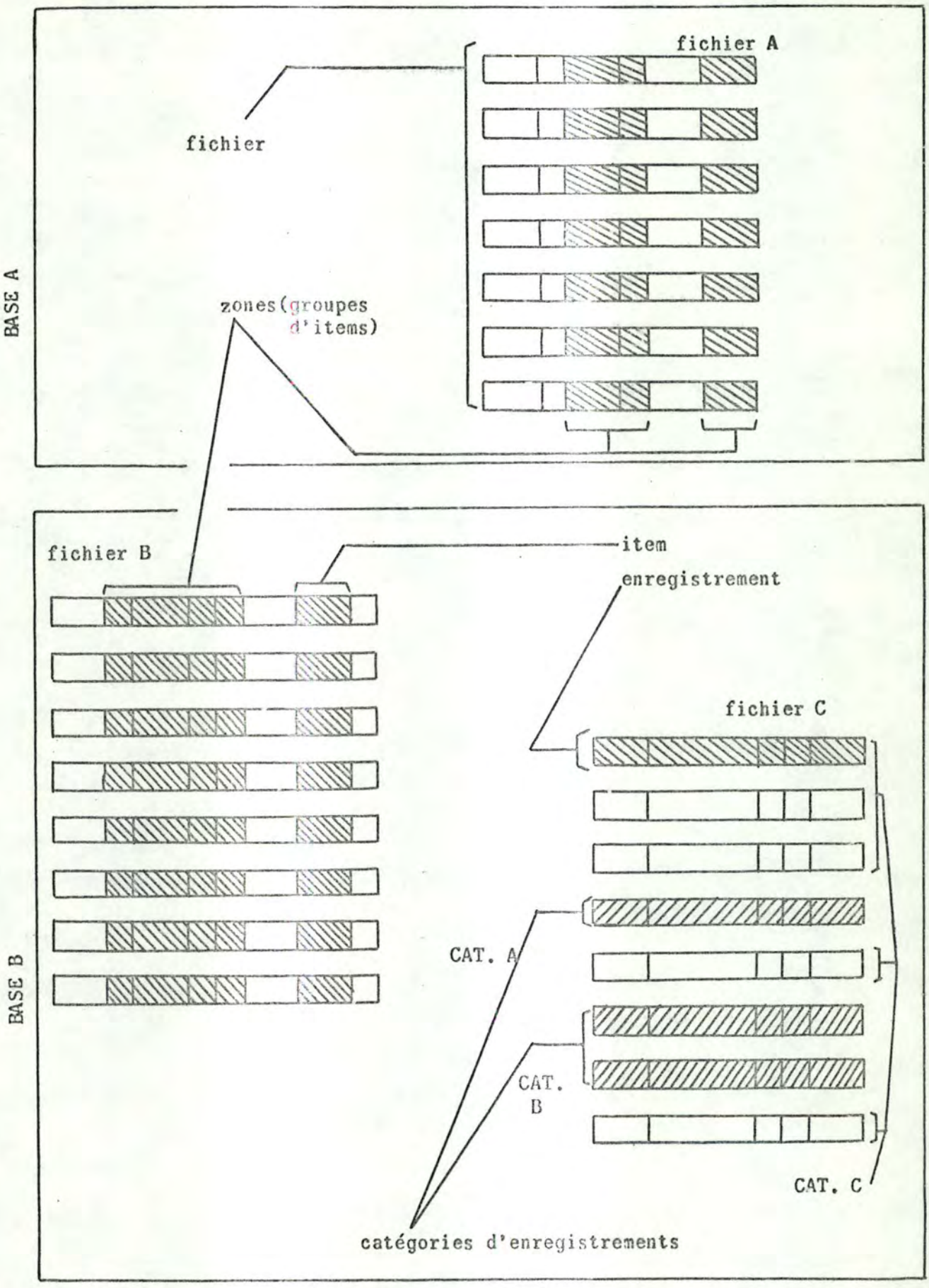

BASE A
fichier
fichier A
zones (groupes d'items)
BASE B
fichier B
item
enregistrement
fichier C
CAT. A
CAT. B
CAT. C
catégories d'enregistrements

fig. 6.2

6.4. TYPES DE STRUCTURES DE TABLES UTILISEES PAR LA FONCTION D'AUTORISATION.

6.4.I. INTRODUCTION.

La fonction d'autorisation peut être réalisée très simplement dans certains cas :
Exemple : Si chaque utilisateur possède ses propres fichiers, la fonction d'autorisation est relativement simple : chaque utilisateur n'a accès qu'à ses fichiers.

Par contre, sur les systèmes utilisant des bases de données, où des informations confidentielles en cotoyent d'autres qui peuvent être divulguées sans aucune restriction, la fonction d'autorisation sera hautement structurée et complexe : une ou plusieurs tables indiqueront les privilèges attribués à chaque utilisateur.

D'une façon générale, la fonction d'autorisation se basera soit :

- sur des niveaux de sécurité,
- sur des entités individuelles ou groupes d'entités,
- ou sur un facteur "temps".

Les entités peuvent être les suivantes :

- les utilisateurs,
- les terminaux ou dispositifs d'entrées/sorties utilisés, (éventuellement d'autres ordinateurs),
- les programmes d'applications,
- les bases de données, fichiers, enregistrements et parties d'enregistrement (items),
- les volumes tels que bandes, ou disques, tambours, sur lesquels les informations (programmes, données) sont conservées.

a) Si des niveaux de sécurité (ou de confidentialité) sont utilisés, on peut assigner l'un de ceux-ci à chacune des entités définies ci-dessus.

b) Une plus grande précision peut être obtenue en se basant sur des entités individuelles ou autres.
Exemple : . tel utilisateur a accès à tels programmes, données et volumes.
. un certain fichier, volume ou programme est déclaré de telle sorte qu'il ne puisse être utilisé que par la personne qui l'a créé.

De tels schémas exigent le recours à des tables d'autorisations hautement structurées. Afin de réduire ces tables, on sera souvent obligé de constituer des groupements de données ou de personnes.

c) Enfin, on peut avoir une fonction d'autorisation se déclenchant automatiquement à certains moments de la journée.

Exemple : . en fin de journée, (en dehors des heures de service), il sera impossible d'accéder à certaines informations même si on dispose du mot de passe ou du code de sécurité correspondant.

Suivant la complexité du système de télétraitement, on sera amené à implémenter l'une des six structures suivantes :

- structure de type "stratification" (ou division horizontale),
- structure de type "compartimentalisation" (ou division verticale),
- structure horizontale et verticale (combinaison des deux précédentes),
- structure en tables d'autorisations,
- structure basée sur l'utilisation de bits d'autorisation à l'intérieur des enregistements,
- structure basée sur l'utilisation de mots-clés, mots de passe ou code sécurité.

La fonction d'autorisation présentée au chapitre III et IV est basée sur une combinaison de ces différents types de structures. Le chapitre IV présente un exemple d'implémentation de cette fonction.

6.4.2. STRATIFICATION.

6.4.2.I. DEFINITION : consiste en une division horizontale en niveaux de sécurité.
Un niveau de sécurité désigne le caractère ou le statut de confidentialité d'un objet. (Nous emploierons aussi le terme : niveau de confidentialité).

Exemples de niveaux :
- top secret, secret, confidentiel, non classé.... ou encore :
- réservé à la direction, d'ordre intérieur....

6.4.2.2. APPLICATIONS :

La division horizontale peut être appliquée aux objets ou entités qui concernent :

I. Le centre informatique : c'est-à-dire :

- les programmes :

Exemple :.utilisation d'une procédure spéciale pour pouvoir lancer un programme dont le niveau de sécurité est élevé.

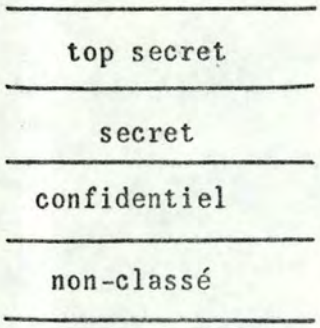
.tout programme ne peut accéder à des données d'un niveau de sécurité plus élevé que le sien.

- les volumes : (disques, bandes, tambours) contenant des données ou des programmes :
Exemple :.le niveau de sécurité indiqué sur ceux-ci sera celui des données ayant le plus haut niveau de sécurité de tout le volume,

.si un volume n'est pas déclaré "secret",des données déclarées "secrètes" ne pourront être transférées sur celui-ci.

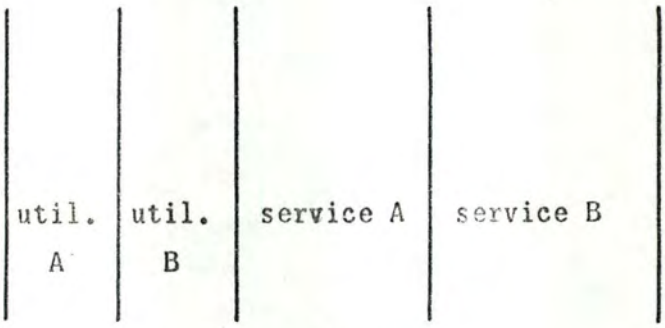
- les opérateurs et pupitreurs :

Exemple :.Un opérateur sera désigné pour monter tout volume déclaré "TOP SECRET" sur une armoire à disque verrouillée par un dispositif hardware quelconque.



STRATIFICATION

fig. 6.4.2

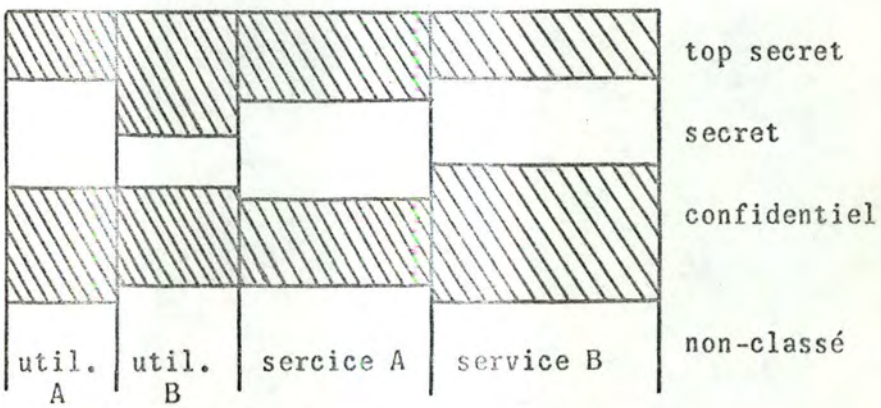


COMPARTIMENTALISATION

fig. 6.4.3

DIVISION VERTICALE ET HORIZONTALE

fig. 6.4.4



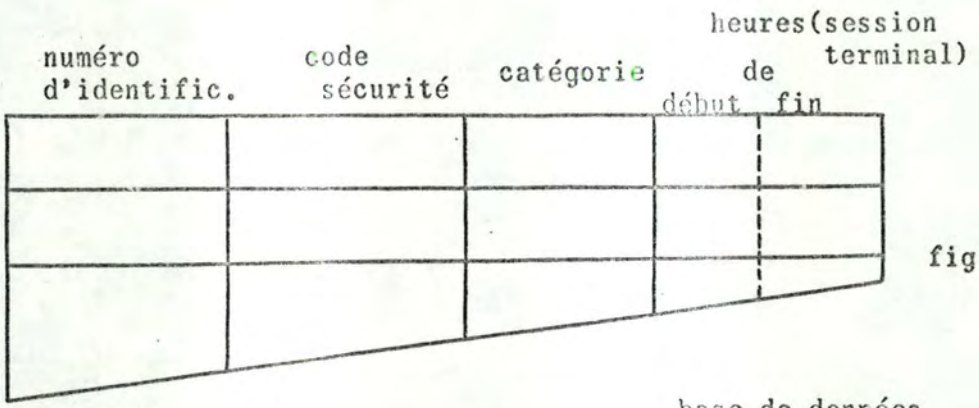


fig. 6.4.5.3$_a$

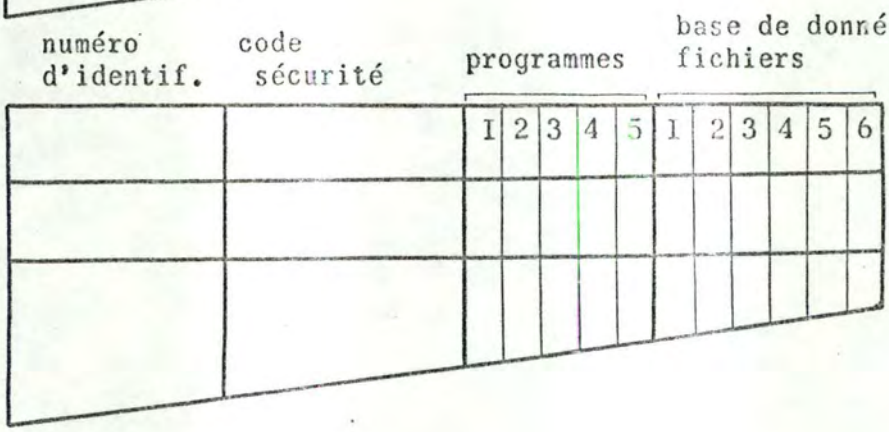


fig. 6.4.5.3$_d$

2. Le réseau de communications : c'est-à-dire :

- les terminaux :

  Exemple : les terminaux ne possédant aucun dispositif de sécurité ne pourront être utilisés pour traiter des données confidentielles.

- les utilisateurs de terminaux :

  Exemple :.les salles ordinateurs et de terminaux ne peuvent être accessibles qu'à des personnes de confiance

  . si l'utilisateur n'est pas autorisé à manipuler des informations déclarées "secrètes", il ne pourra pas utiliser un terminal désigné pour les travaux "secrets" ainsi que tout programme, donnée ou volume déclaré "secret".

- le personnel : (excepté les utilisateurs)

  Exemple : aucune personne n'est autorisée à examiner des documents, données ou programmes d'un niveau de sécurité supérieur au sien.

- les listings et feuilles console :

  . chaque page comportera un numéro de suite (pour s'assurer qu'aucune n'a été perdue).
  (remarquons qu'il est toujours possible d'interposer un carton entre la feuille console et le dispositif d'impression, lors de l'introduction d'une transaction non-autorisée; d'où la nécessité d'enregistrer toute transaction entrée dans le système (logging).

Le nombre de niveaux de sécurité dépend, en pratique, du caractère "sensible" (confidentiel) des données.

6.4.3. COMPARTIMENTALISATION.

6.4.3.1. DEFINITION : consiste en une division verticale entre différents utilisateurs ou départements. Exemple (voir Fig. 6.4.3.)

6.4.3.2. APPLICATION :

Lors de sa mise en place dans un système, il est nécessaire d'obtenir des séparations très nettes entre les compartiments, soit, par exemple : l'utilisateur A (Fig. 6.4.3.) ne doit pas être capable d'accéder aux données et programmes de l'utilisateur B.

Ce type de structure est applicable sur les systèmes de télétraitement quand des jobs différents peuvent tourner concurremment dans différentes partitions.
Exemple : cas où les jobs ont des exigences de sécurité fort différentes.

6.4.4. STRUCTURE HORIZONTALE ET VERTICALE (voir Fig. 6.4.4.)

Par contrôle software, on peut élaborer des codes d'accès qui limitent différentes catégories d'utilisateurs à différents niveaux d'informations plus ou moins secrètes.
L'operating system (programme de contrôle) joue ici un rôle important dans le maintien de la sécurité.

6.4.5. STRUCTURE EN TABLES D'AUTORISATION.

6.4.5.1. INTRODUCTION.

La nécessité d'élaborer des structures plus complexes est due aux faits suivants :

I) les mêmes données ou programmes peuvent être partagés entre plusieurs utilisateurs.
Exemple : un même item peut n'être accessible qu'à certaines personnes.
(Rappelons que l'item est la plus petite partie de l'enregistrement ayant encore une signification : par exemple, un nom, le code postal d'une adresse. C'est en somme, la structure de donnée la plus élémentaire.)

2) une base de donnée peut être employée pour de multiples objectifs : consultation, mise à jour, relevé statistique...

6.4.5.2. DEFINITION.

Les tables d'autorisation indiquent les données et les programmes que chaque utilisateur est autorisé à manipuler et sont consultées par la fonction d'autorisation.

Si l'on représente par un réseau l'ensemble des relations entre transactions, programmes et données, (voir Fig. 6.4.5.2.) un des privilèges accordé (par la table d'autorisation) à l'utilisateur peut être considéré comme un chemin dont les étapes (sommets) seront successivement : un utilisateur, un code transaction, un programme d'application, (un ou plusieurs sous-programmes ou fonctions élémentaires), une base de données, un ou plusieurs fichiers de cette base, un ensemble d'enregistrements, un ou plusieurs items à l'intérieur de chaque enregistrement.

Le responsable de la sécurité peut ainsi accorder plusieurs privilèges à chaque utilisateur, ce qui correspond à définir un arbre à l'intérieur du réseau de la Fig. 6.4.5.2.

6.4.5.3. DIFFERENTES FORMES DE TABLES D'AUTORISATION.

a) Répartition des utilisateurs en catégories.

PRINCIPE : L'ensemble des utilisateurs est divisé en un petit nombre de catégories. Les privilèges accordés à l'utilisateur dépendront de sa catégorie. Remarquons que tous les utilisateurs appartenant à une même catégorie ont les mêmes privilèges.

STRUCTURE : Pour chaque utilisateur, une entrée de la table comportera par exemple :
- un n° d'identification,
- un code sécurité ou mot de passe,
- la catégorie de l'utilisateur. (voir Fig. 6.4.5.3 a)

Lors de la procédure d'autorisation, la catégorie sera déterminée soit :
- par le mot de passe, le code sécurité, le badge ou la carte qu'il introduit au terminal,

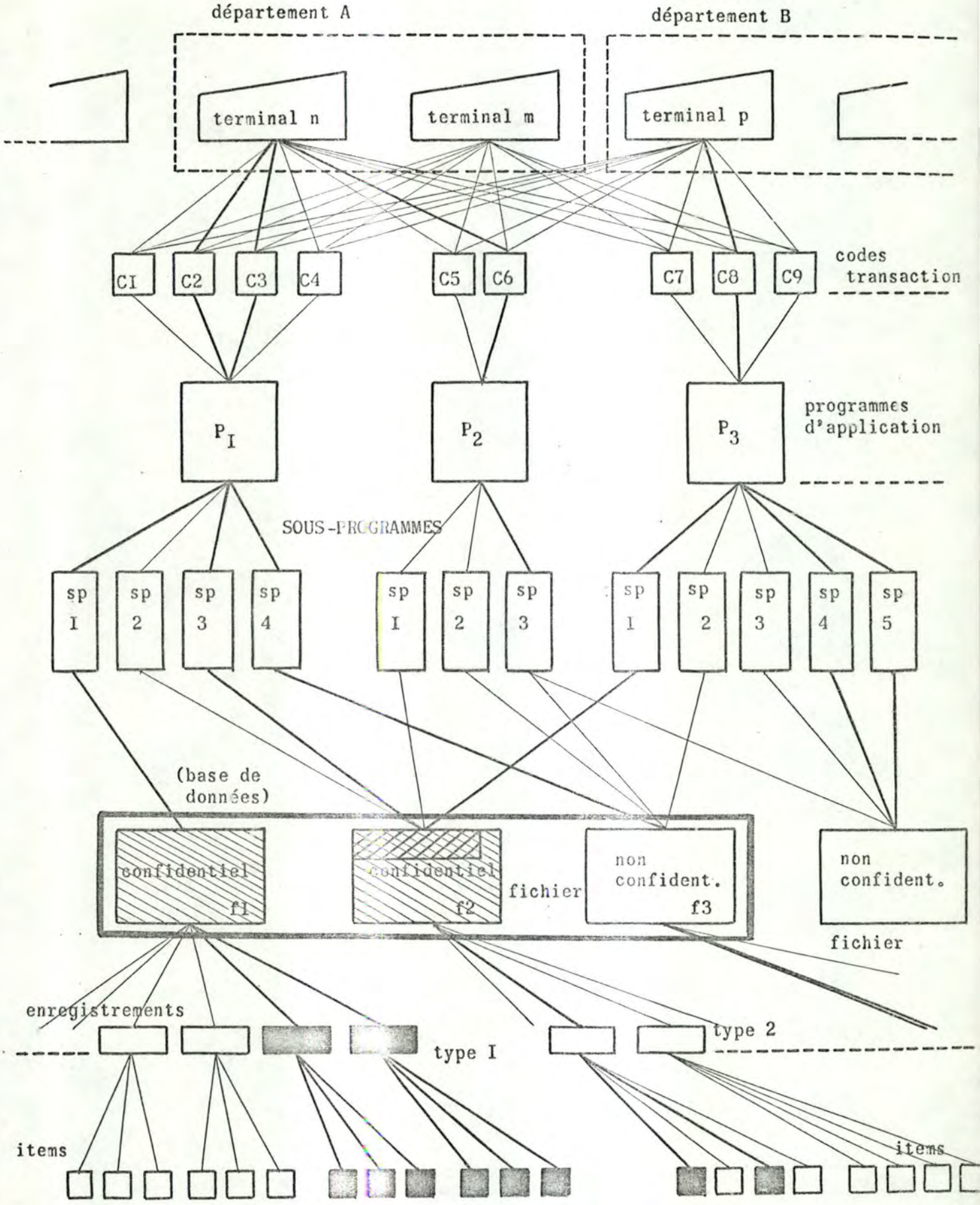

département A
département B
terminal n
terminal m
terminal p
C1
C2
C3
C4
C5
C6
C7
C8
C9
codes transaction
P1
P2
P3
programmes d'application
SOUS-PROGRAMMES
sp 1
sp 2
sp 3
sp 4
sp 1
sp 2
sp 3
sp 1
sp 2
sp 3
sp 4
sp 5
(base de données)
confidentiel f1
confidentiel f2
fichier
non confident. f3
non confident.
fichier
enregistrements
type I
type 2
items
items

fig. 6.4.5.2

- par l'adresse du terminal lui-même ou par sa localisation,
- par un algorithme exploitant le code de sécurité introduit.

EXEMPLE : Système de réservation de place dans une compagnie aérienne ; le badge qui sert à l'utilisateur pour son identification indique aussi sa catégorie : employé, hôtesse, démonstrateur, douanier .... (voir Fig. 6.4.5.3 c).

système bancaire : l'insertion d'une clé spéciale dans une serrure placée sur le terminal permet à l'utilisateur d'accéder aux données confidentielles. (voir Fig. 6.4.5.3. b).

b) Systèmes basés sur les individualités de chaque utilisateur.

PRINCIPE : La catégorie d'autorisation est remplacée par l'indication des autorisations de chaque utilisateur.

STRUCTURE : Chaque entrée de la table d'autorisation peut comporter les indications suivantes :(voir Fig. 6.4.5.3. d)

1. Programmes qui peuvent être utilisés,
2. Types de transactions qui peuvent être entrées,
3. Fichiers qui peuvent être lus,
4. Fichiers qui peuvent être modifiés.
5. Catégories de données d'un fichier qu'un utilisateur peut lire,
6. Catégories de données qu'un utilisateur peut modifier.

EXEMPLES

a) Une entrée de la table correspond à un utilisateur. Chaque entrée pourra, par exemple, indiquer les types de transactions que ce dernier peut entrer. Cette table est représentée à la fig. 6.4.5.3. e. Les parties "numéro de l'utilisateur" et "code sécurité" seront exploitées par la fonction d'identification de l'utilisateur. Le vecteur des bits d'autorisation servira à la fonction d'autorisation, lors de chaque transaction. Le vecteur comporte un seul bit par transaction.

Les parties(I) et (2) seront utilisées par la fonction d'identification :

- soit à chaque initialisation d'une session termina
- soit en cours de session, à chaque entrée de transaction, pour certifier, d'une transaction à une autre, que l'utilisateur est bien celui qui a initialisé la session.

b) La Fig. 6.4.5.3. f représente une table d'autorisation qui utilise trois bits pour chaque type de transaction :

- bit indiquant si l'utilisateur est autorisé à modifier chaque enregistrement concerné par la transaction ; (4)
- bit indiquant s'il a suffisamment d'expérience pour mettre à jour réellement le fichier (le fichier sera donc physiquement modifié) ; (5)
  Ceci permet de tester des programmes en utilisant une base de données réelle.
- bit donnant à l'utilisateur l'autorisation de lire chaque enregistrement concerné par la transaction (3)

c) Il est possible de codifier les types d'autorisation à l'aide de deux bits; soit la convention suivante :

00 = aucune permission
01 = lecture uniquement
10 = mise à jour (phase de test)
11 = mise à jour (phase d'exploitation)

PROCEDURE : Avant d'exécuter le(s) programme(s) permettant de traiter une transaction, le programme de contrôle d'accès balaye cette table d'autorisation. Pour pouvoir par exemple lire un fichier l'utilisateur doit :

. introduire le code de sécurité correct,
. avoir l'autorisation de lire ce fichier.

REMARQUES :-La table représentée à la Fig. 6.4.5.3. e peut se rapporter à des types de transactions ou aux programmes traitant celles-ci. Dans le premier cas, l'utilisateur ne pourra entrer tous les types de transaction reconnus par le programme auquel il a accès; il ne pourra donc accéder qu'à certaines parties du programme.

Dans le second cas, l'autorisation porte sur le programme d'application et non plus sur les types de transactions qu'il peut traiter, ce qui implique que l'utilisateur peut entrer tous les types de transaction se rapportant au programme auquel il a accès. (voir Fig. 6.4.5.2.).

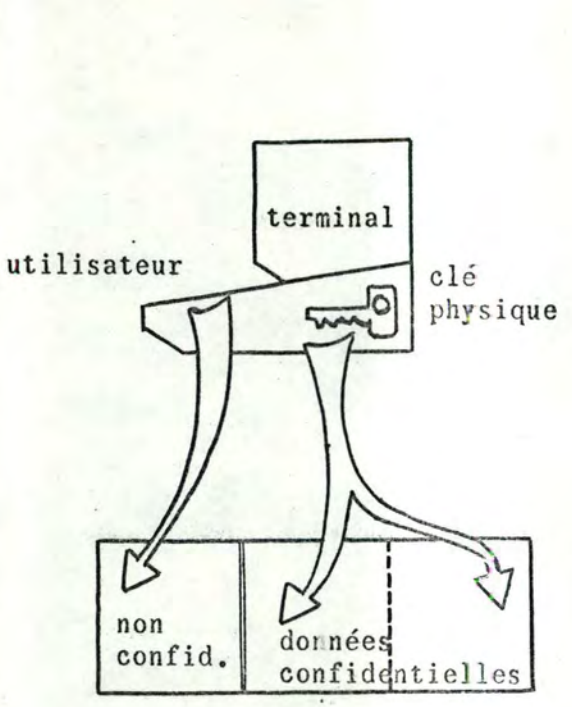
-Le chapitre III présentera un exemple de programme d'accès ainsi que les tables de sécurité qui s'y rapportent. On trouvera les résultats de son implémentation au chapitre IV.

EXTENSION : En général, les tables d'autorisation seront résidentes en mémoire centrale; toutefois, si le nombre d'utilisateurs, de programmes, de fichiers ou de transactions augmente, il peut être avantageux, du point de vue gain de place en mémoire centrale, de travailler directement à partir de la table sur disque. Celle-ci se présente alors sous la forme d'un fichier dont chaque enregistrement correspond à une entrée de la table.

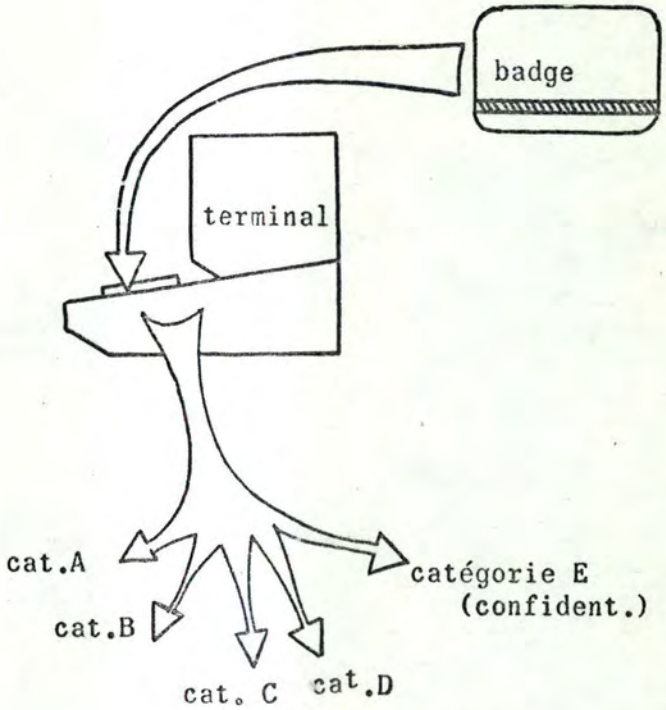
Principe : Pour chaque utilisateur, on crée un enregistrement contenant :
- son numéro d'identification,
- son code de sécurité,
- 2 bits par type de transaction.

Procédure de contrôle d'accès :

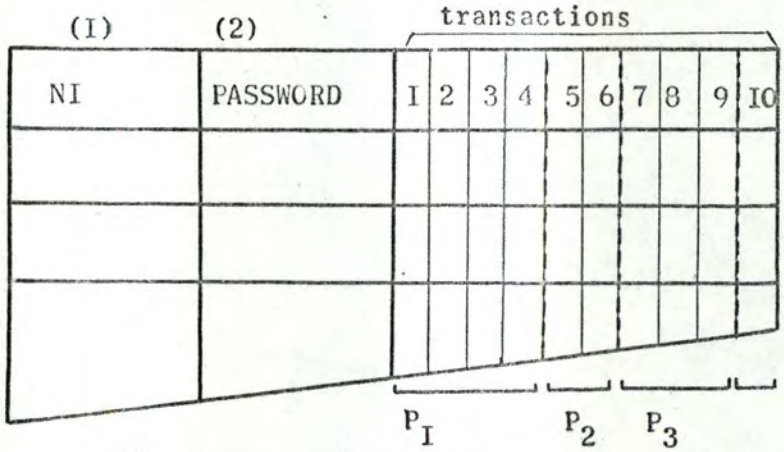
Dès que l'utilisateur a introduit son numéro d'identification, son enregistrement est lu à partir du fichier (table) mémorisé sur un cylindre ou sur tout un diskpack si la base est assez vaste. Le temps d'accès moyen est de quelques dizaines de millisecondes.



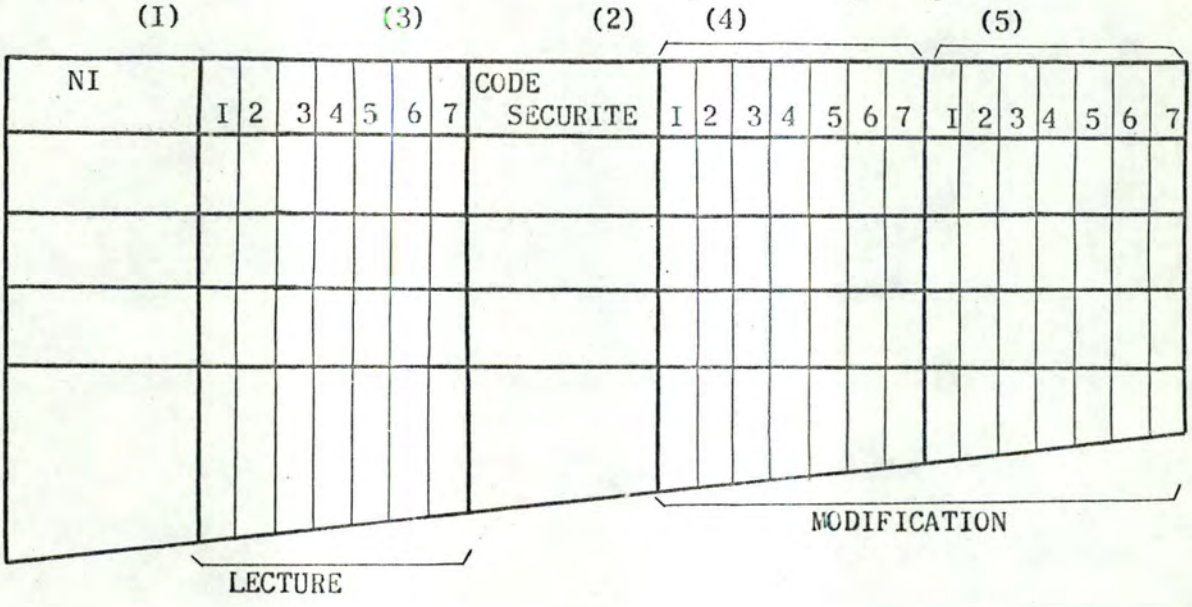
(b)



(c)



(e)



(f)

fig. 6.4.5.3

CONCLUSIONS :

Jusqu'à présent, les tables d'autorisation ne se sont basées que sur les types de transaction de chaque programme d'application, ce qui nous a permis de contrôler l'accès soit aux programmes, soit aux enregistrements des fichiers nécessaires aux programmes de traitement des transactions.
La première solution consistait à dire : "l'utilisateur peut utiliser ou non telle transaction". Il fallait un bit par type de transaction.

La seconde solution allait plus loin : Le fichier concerné par la transaction peut ou non être lu, modifié physiquement ou modifié pour les besoins d'un test sans que le fichier le soit physiquement.

- Chaque type de transaction ou chaque programme utilise soit un enregistrement, un groupe d'enregistrements appartenant à un même fichier ou à des fichiers ≠. Si l'on désire que l'utilisateur n'ait accès qu'à certains enregistrements, les tables d'autorisation deviennent alors considérables et de ce fait, peu pratiques. Afin de réduire leur dimension, on peut procéder à certains groupages.

c) Groupements d'utilisateurs, groupement de données.

PRINCIPE : Un groupe comprend tous les utilisateurs qui ont des privilèges identiques ; chaque groupe (et non plus chaque utilisateur) est associé à une entrée de la table d'autorisation.

Exemple : Tous les employés d'un bureau seront répertoriés comme faisant partie d'un même groupe.

On peut, de même, effectuer des groupements d'enregistrements.

Exemple : Le fichier du personnel pourrait être groupé,

- soit par département,
- soit par rang (manager du premier niveau, manager du second niveau),
- soit par catégorie de zone (traitement, appréciation, etc....)

STRUCTURE : La Fig. 6.4.5.3. g représente les tables d'autorisations utilisées dans le cas de groupement de données et d'utilisateurs.

Nous adopterons la forme de table des groupes présentée ici, lorsque chaque groupe d'utilisateurs peut accéder à presque tous les enregistrements.

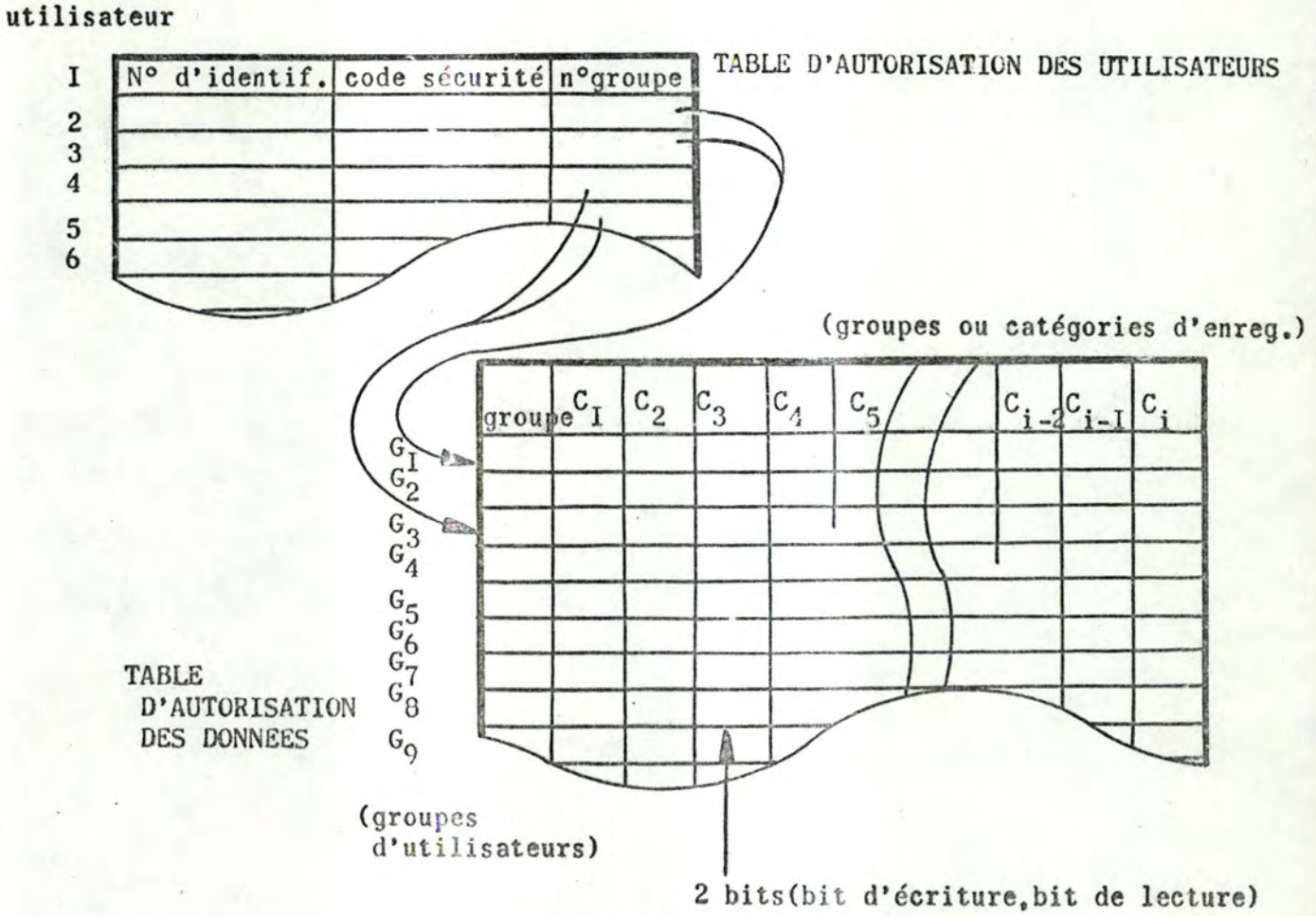
Si, par contre, la plupart des groupes d'utilisateurs ne peuvent accéder qu'à quelques groupes de données, il sera préférable d'adopter une forme semblable à celle présentée au chapitre III.

PROCEDURE DE CONTROLE D'ACCES :

(voir organigramme de la page suivante).

EXEMPLE D'UTILISATION :

(voir chapitre III et IV).



Conventions:

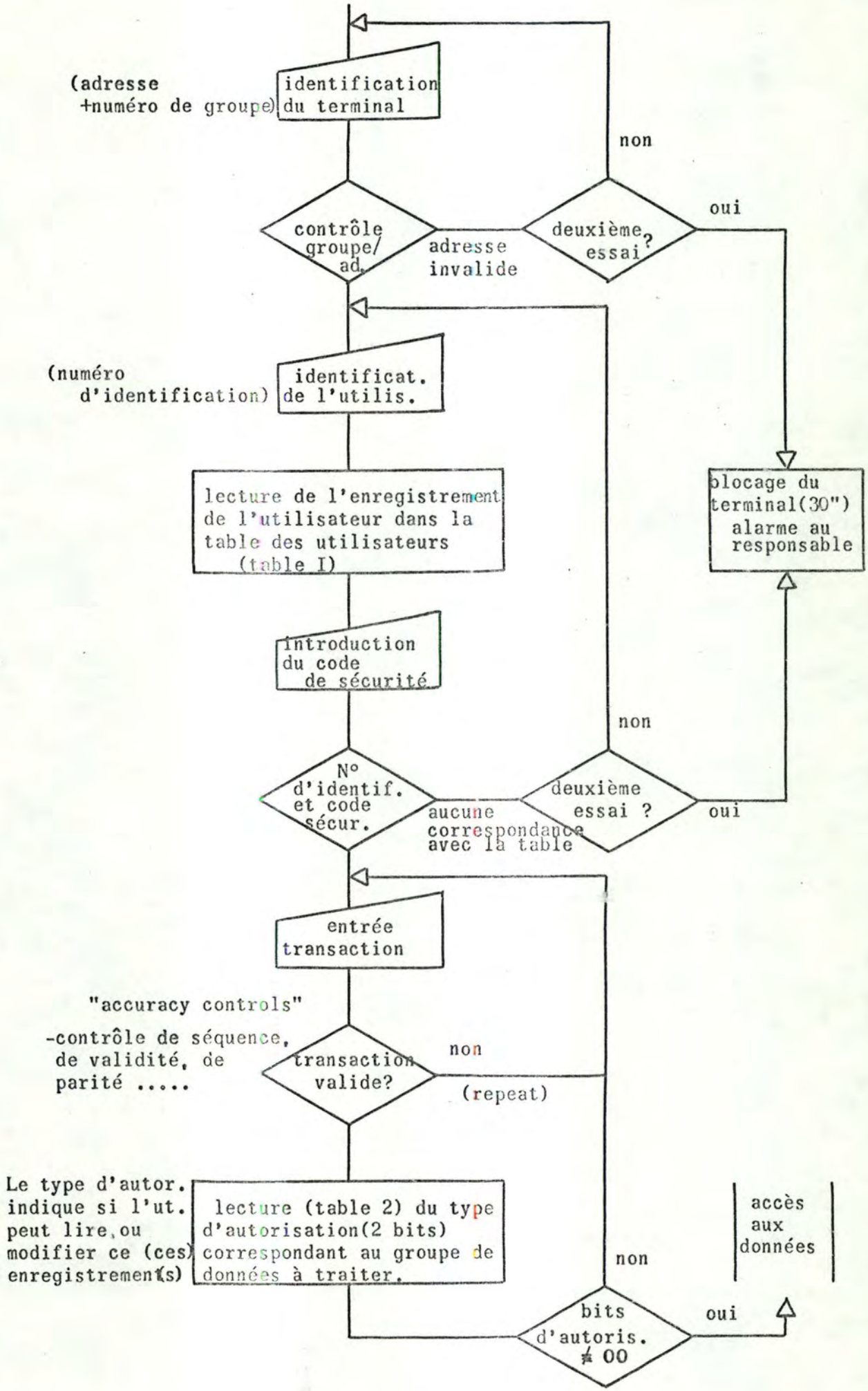
00 : aucune permission

01 : lecture uniquement(bit de lecture "ON"

11 : lecture et écriture

10 : écriture uniquement(bit d'écriture "ON"

fig. 6.4.5.3 (g)


(adresse +numéro de groupe)
identification du terminal
non
contrôle groupe/ ad.
adresse invalide
deuxième essai?
oui
(numéro d'identification)
identificat. de l'utilis.
lecture de l'enregistrement de l'utilisateur dans la table des utilisateurs (table I)
blocage du terminal(30") alarme au responsable
introduction du code de sécurité
non
N° d'identif. et code sécur.
aucune correspondance avec la table
deuxième essai ?
oui
entrée transaction
"accuracy controls"
-contrôle de séquence, de validité, de parité .....
transaction valide?
non
(repeat)
Le type d'autor. indique si l'ut. peut lire, ou modifier ce (ces) enregistrement(s)
lecture (table 2) du type d'autorisation(2 bits) correspondant au groupe de données à traiter.
accès aux données
non
bits d'autoris. ≠ 00
oui

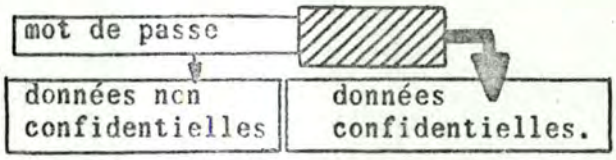
6.4.6. STRUCTURE BASEE SUR L'UTILISATION DE MOTS-CLES, MOTS DE PASSE OU CODES SECURITE

6.4.6.I. MOTS DE PASSE ASSOCIES AUX FICHIERS.

Appliquée au niveau de l'identification de l'utilisateur d'un terminal, (voir section 5), la technique des mots de passe ne permettait pas d'assurer une protection absolue contre tout accès au système.

Appliquée aux fichiers, elle permet à l'utilisateur d'un terminal :

- de verrouiller ses propres fichiers (que lui seul utilise) à l'aide de mots de passe qu'il est seul à connaître et qu'il peut modifier à tout instant,
- de verrouiller ses propres fichiers au moyen de mots de passe qu'il communique à tous les utilisateurs qui peuvent les consulter (accès partagé); En principe, il est le seul à pouvoir modifier les enregistrements de ses fichiers.
  En fait, en ajoutant un préfixe ou un suffixe (fourni par le propriétaire) au mot de passe, certains utilisateurs pourront modifier le fichier ou accéder aux données confidentielles.



Dans la majorité des cas, cette protection sera suffisante sans pour autant être absolue : un utilisateur ingénieux ou persévérant pourra toujours obtenir le mot de passe (ex : introduction répétée de mots de passe (lockword experimentation) générés automatiquement par un mini-ordinateur.)

Dans un contexte fichier, on peut associer un mot de passe soit

- à une base de données,
- à un fichier de cette base,
- à un groupe ou une catégorie d'enregistrements,
- à un enregistrement individuel,
- à un ensemble d'items à l'intérieur de tous les enregistrements d'un même fichier,
- à un ensemble d'items à l'intérieur de tous les enregistrements d'une même catégorie.

Remarque :

. Un fichier ne nécessitant aucune protection pourra être déclaré par son propriétaire comme "commun", c'est-à-dire disponible à l'ensemble des utilisateurs (aucune restriction);

. Si la technique des mots de passe est la seule utilisée pour assurer la protection d'une base de données ou de ses fichiers, il est souhaitable d'établir une distinction très nette entre les ≠ niveaux de confidentialité des données,

. Plutôt que de permettre à l'utilisateur d'assumer lui-même la protection en générant les mots de passe de ses propres fichiers l'assignation, le contrôle et la maintenance de ceux-ci peut être exécutée par une seule personne pour tous les utilisateurs.

L'administrateur de la sécurité du système ou responsable de la sécurité.

6.4.6.2. EXTENSION DE LA TECHNIQUE DES MOTS DE PASSE.

PRINCIPE : Utilisation de la technique des mots de passe conjointement à celle des tables d'autorisations pour obtenir un haut degré de sécurité.

APPLICATIONS : En dehors du contexte "fichiers", un mot de passe pourra être associé soit :

- à un seul utilisateur (identification),
- à une catégorie d'utilisateurs, c'est-à-dire l'ensemble des personnes ayant accès aux mêmes données :
  Exemple ; un service.

  Remarque : cette solution présente l'inconvénient suivant: chaque fois qu'un utilisateur change de groupe, le mot de passe du groupe de départ doit être modifié.
- à un programme d'application,
- à un terminal ou à son emplacement,
- à une combinaison de ceux-ci.

6.4.7. BITS D'AUTORISATION.

Outre l'utilisation de tables d'autorisations ou/et de mots de passe, la protection de la base de données peut être également réalisée en insérant des bits d'autorisation dans chacun de ses enregistrements.

Chaque bit d'autorisation peut avoir trait soit : (voir Fig. 6.4.7.)

(a) - à un utilisateur,
(b) - à un groupe ou une catégorie d'utilisateurs,
(c) - à un niveau de sécurité,
(d) - à un programme d'application,
(e) - à un terminal (ou son emplacement).

Remarquons que cette technique entraîne un accroissement du nombre d'accès disque : l'enregistrement est amené en mémoire, même si l'utilisateur n'y a pas accès. Vu la difficulté de mise à jour, la technique d'insertion de bits d'autorisation dans chaque enregistrement de la base de données ne doit être utilisée que si le nombre d'utilisateurs, de catégories, de niveaux de sécurité, de programmes, de terminaux et d'enregistrements de la base de données (suivant la signification des bits) est peu élevé et relativement fixe.

En pratique, la protection au niveau de l'enregistrement peut utiliser des codes ou des bits d'autorisation implémentés soit :

. dans les enregistrements eux-mêmes (voir Fig. 6.4.7),
. dans la directory utilisée pour adresserles enregistrements,
. dans une table séparée (exemple : tables du programme de contrôle d'accès développé au chapitre III).

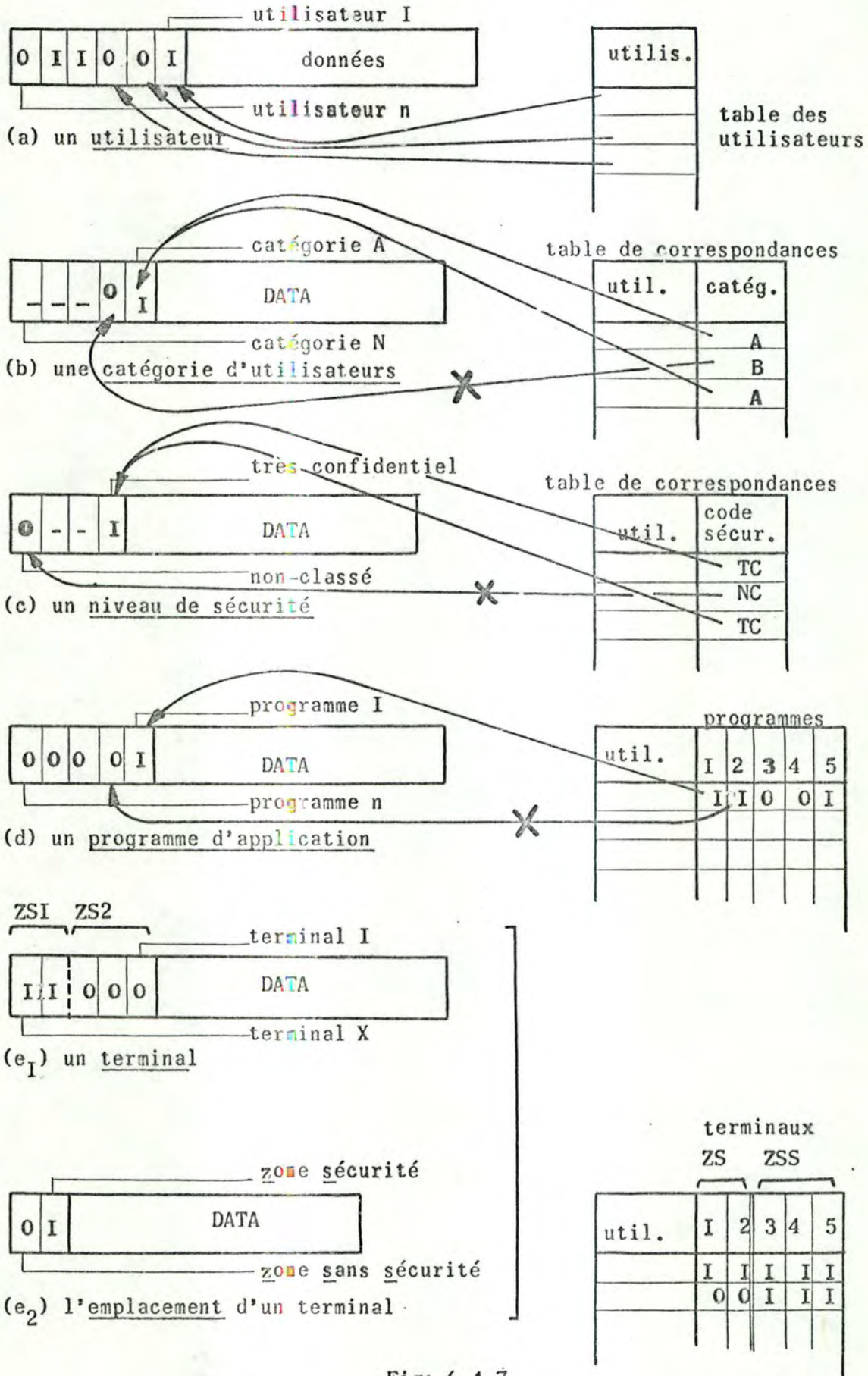

Conventions: -bit = 0:aucun accès
-bit = I: accès aux données
utilisateur I
0 I I 0 0 I
données
utilisateur n
(a) un utilisateur
utilis.
table des utilisateurs
catégorie A
_ _ _ 0 I
DATA
catégorie N
(b) une catégorie d'utilisateurs
table de correspondances
util.
catég.
A
B
A
très confidentiel
0 - - I
DATA
non-classé
(c) un niveau de sécurité
table de correspondances
util.
code sécur.
TC
NC
TC
programme I
0 0 0 0 I
DATA
programme n
(d) un programme d'application
programmes
util.
1 2 3 4 5
I I 0 0 I
ZSI ZS2
terminal I
I I 0 0 0
DATA
terminal X
(e1) un terminal
zone sécurité
0 I
DATA
zone sans sécurité
(e2) l'emplacement d'un terminal
terminaux
ZS ZSS
util.
I 2 3 4 5
I I I I I
0 0 I I I

Fig: 6.4.7

6.5. PROCEDURES D'AUTORISATIONS PARTICULIERES.

Sur certains systèmes, la procédure d'autorisation peut être extrêmement complexe. L'autorisation d'accéder à un enregistrement peut dépendre soit :

I. du contenu de l'enregistrement ou du résultat du traitement des données de cet enregistrement :

Exemple : Un utilisateur peut obtenir la valeur de l'item "salaire" des enregistrements d'une base de données concernant le personnel à condition que cette valeur ne dépasse pas 25;000 francs.

2. de la forme sous laquelle une question est posée ;

Exemple : L'utilisateur peut accéder à un enregistrement donnant le nombre de maladies graves d'une personne; il peut ne pas obtenir ce nombre mais simplement être renseigné sur le fait que la personne a bien été malade ou non.

3. de la relation entre certains items :

Exemple : Des chercheurs peuvent utiliser une base de données médicales. Chaque enregistrement contient :

- le nom du patient,
- l'âge,
- des détails médicaux portant sur les maladies antécédantes du patient.

Les chercheurs pourront obtenir soit les noms des patients ainsi que leur âge ou soit les détails médicaux uniquement. En aucun cas, ils ne peuvent être capables d'associer les détails médicaux correspondants à un nom. Ceci suppose qu'ils n'obtiendront pas la liste des noms dans le même ordre que celle des détails médicaux.

6.5.I. PROCEDURES BASEES SUR LE CONTENU DE L'ENREGISTREMENT.

Lorsque l'autorisation doit être basée sur les valeurs d'items ou combinaisons de valeurs, un ensemble d'expressions de qualification peuvent être stockées pour chaque fichier; le programme de contrôle aura la tâche de lire les données demandées, d'appliquer les expressions de qualification à celles-ci et de décider si certains items doivent être supprimés, modifiés ou tronqués avant d'être retournés au programme d'appliquation. La nature des expressions de qualification (exemple : table de décisions) dépendent du programme d'application.

6.5.2. BASE DE DONNEES STATISTIQUES.

L'autorisation d'accès basée sur la forme sous laquelle une question est posée ou sur la relation entre certains items concerne les banques de données utilisées à des fins statistiques où une multitude de questions peuvent être posées. (Statistical data base)

DEFINITION :

Dans une base de données statistiques (destinée à des opérations statistiques), l'utilisateur peut balayer tous les enregistrements mais est incapable d'associer les faits à un individu déterminé. Il peut toutefois obtenir des ensembles de valeurs et des corrélations.

LE PROBLEME :

De telles bases de données, l'utilisateur peut parfois déduire des informations qu'il n'est pas autorisé à connaître en posant des questions d'une certaine manière.

EXEMPLE :

Supposons que l'utilisateur souhaite trouver le revenu d'une personne dont il connaît certaines caractéristiques.
Il peut poser une série de questions en ajoutant chaque fois une nouvelle caractéristique, de façon à réduire successivement la taille de l'échantillon.
Dans cette procédure, un facteur très rare (comme la taille, un poids élevé ou la nationalité) peut diminuer le temps de recherche.
Si l'échantillon de départ est réduit (après une série de questions), à un effectif, l'utilisateur pourra poser d'autres questions sur la personne en utilisant toujours les mêmes paramètres + une condition supplémentaire.

Il est ainsi possible de trouver des informations sur un individu précis dont on connaît certaines caractéristiques même si le nom ou d'autres caractéristiques sont absentes de la base ou rendues inaccessibles. (voir techniques cryptographiques).

SES SOLUTIONS :

L'autorisation d'accès doit ici être basée sur :

- les résultats des recherches de l'utilisateur,
- la taille de l'échantillon qu'il prend en considération,
- les activités précédentes.

a) autorisation basée sur les résultats des recherches : exemples :

- possibilité d'obtenir des valeurs comme la moyenne ou la la déviation standard mais pas de valeurs explicites,
- impossibilité de demander la valeur minimum et maximum de certains items.

b) autorisation basée sur la taille de l'échantillon :

- empêcher toute réponse fournie par le système si la dimension de l'échantillon est trop faible, la taille minimum de l'échantillon utilisé pouvant différer d'un fichier à l'autre.

c) autorisation basée sur les activités précédentes :

- un ensemble de toutes les activités de l'utilisateur peut être conservé et utilisé statistiquement.
  Exemple : activité où l'utilisateur pose plusieurs questions similaires.
  Par des contrôles fréquents, on découragera les utilisateurs de se transformer en intrus.

6.6. CONCLUSIONS.

a) l'utilisation de tables de sécurité dont la structure est complexe augmentera le nombre d'instructions de la fonction d'autorisation (routines de calcul d'adresse, de recherche en table ...) et d'une façon générale, l'overhead du système de sécurité (fonction d'identification et d'autorisation).

En pratique, le choix de la structure des tables résultera d'un compromis entre d'une part, le degré de sécurité à obtenir et d'autre part, l'occupation mémoire et les facilités d'utilisation de celles-ci. L'occupation mémoire étant proportionnelle au nombre de terminaux, d'utilisateurs, de programmes et de fichiers de la base de données (éventuellement du nombre de bases de données).

b) Avant chaque accès au système (terminaux, programmes, données) :

- l'ensemble du mécanisme de contrôle d'accès sera invoqué ; ceci comprend le cas d'un accès au mécanisme lui-même (maintenance du mécanisme).

c) Lors de chaque appel à ce mécanisme, celui-ci doit :

- s'assurer qu'il n'a pas été modifié par une personne autre que le responsable de la sécurité;
- vérifier l'identité de l'utilisateur qui a provoqué la demande d'accès.

d) Le mécanisme peut être implémenté à quatre endroits différents :

- lors de la réalisation du système d'exploitation ou du programme de contrôle en l'incluant intégralement à celui-ci ;
- par additions ou modifications à un operating system ne comportant aucun dispositif de protection ;
- en l'incluant entièrement dans les programmes d'application (sous forme d'un moniteur au début de chaque programme) ;
- en l'incluant au niveau du système de gestion de bases de données (recommandations du DBTG du CODASYL).

e) Il est, de plus, souhaitable que le responsable de la sécurité puisse modifier les autorisations en temps réel au moyen d'un langage de mise à jour. (voir langage "LAMA" développé et implémenté aux chapitres III et IV).

section 7 : techniques cryptographiques appliquées à la sécurité des données.

7.1. INTRODUCTION.

Les constructeurs se penchent actuellement sur des systèmes permettant d'obtenir un degré de sécurité satisfaisant, au moindre coût, tout en augmentant celui de l'obtention illégale de données à un degré tel qu'elle ne serait plus rentable du point de vue économique, vu les moyens à mettre en oeuvre (mini-ordinateur, implémentation de la procédure d'identification utilisée sur un autre système, étude empirique).

Les dispositifs cryptographiques peuvent contribuer à la sécurité des données introduites ou conservées dans un système fonctionnant en télétraitement et utilisant une ou plusieurs bases de données.

L'utilisateur d'un tel système doit pouvoir s'assurer que l'ordinateur qu'il utilise est effectivement le sien. De son côté, l'ordinateur doit pouvoir se protéger contre un instrus habile voulant accéder au système. Il faut aussi pouvoir s'assurer de l'intégrité des messages entrés et des données de la base. Chacun de ces cas peut être résolu par l'application d'une technique cryptographique. Toutefois, si ce type de protection est adopté, il doit être soumis à des impératifs d'efficacité (dans le sens de difficulté de déchiffrement d'un cryptogramme).

7.2. TECHNIQUES CRYPTOGRAPHIQUES.

7.2.I. DEFINITION.

Une technique cryptographique : permet l'encodage/décodage (ou chiffrement/déchiffrement) d'un texte en clair ("plaintext")/cryptogramme.

Un cryptogramme : un message écrit en caractères secrets.

Un chiffre : consiste à transformer les composants élémentaires d'un message (bits ou caractères) en fonction d'une stratégie (algorithme) particulière.

Un code : consiste en une liste conventionnelle donnant la correspondance entre éléments d'un langage naturel et éléments du code, permettant ainsi de représenter par un petit groupe de symboles un mot complet, une transaction ou un message entier.

7.2.2. CLASSES DE TECHNIQUES.

On distingue deux grandes classes de techniques :

- celles qui sont basées sur la substitution des caractères du message avec d'autres caractères,
- celles qui sont basées sur la transposition (modification) de l'ordre des caractères du message.

Les techniques de transformation basées sur la substitution de caractères sont les plus faciles à implémenter en ordinateur, aussi nous ne retiendrons que celles-là dans le cadre de cette étude.

7.2.3. TECHNIQUES DE SUBSTITUTION.

7.2.3.1. SUBSTITUTION MONOALPHABETIQUE. (CAESAR cipher-chiffrement de CAESAR).

Chaque caractère x_i du message en clair est transformé en un caractère y_i du cryptogramme par addition (module N) d'une constante c.

$$y_i = x_i + c \pmod{N}$$

N est la dimension de l'alphabet. (Cet alphabet est, ici, la liste des valeurs de c.) La constante c ne peut prendre que N-I valeurs possibles.

7.2.3.2. SUBSTITUTION POLYALPHABETIQUE de période u (chiffre de Vigenère).

Consiste à appliquer cycliquement u substitutions monoalphabétiques par addition (module N) de u constantes $c_0, c_1, \ldots, c_{u-1}$.

$$\begin{aligned} y_0 &= x_0 + c_0 \\ y_1 &= x_1 + c_1 \pmod{N} \\ &\ldots\ldots\ldots\ldots \\ y_j &= x_j + c_j \pmod{u} \end{aligned}$$

Puisque chaque c_i peut prendre N valeurs possibles, et que d'autre part, la période est u, l'espace des clés contient N^u sélections possibles des constantes $c_0, \ldots c_{u-1}$.

Exemples : voir Fig. 7.2.3.2. a et b.

7.2.3.3. SUBSTITUTION POLYALPHABETIQUE A k BOUCLES.

Applique cycliquement k ensembles d'alphabets, avec des périodes $u_1, \ldots, u_k$.

$$y_j = x_j + c_{1,J} \pmod{u_1} + \ldots\ldots + c_{k,j} \pmod{u_k} \pmod{N}$$

TEXTE CLAIR COMEHERE

CLE(EXIT) EXITEXIT

TEXTE CHIFFRE GLUXLBZX

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Chiffrement de Vigenère obtenu en établissant une correspondance bi-univoque entre caractères du texte clair et caractères de la clé. La clé est répétée en totalité (période) ou en partie en fonction des besoins.

									10		12		14		16		18		20		22		24			
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	G	H	I	J	K	L	M	N	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
7	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Chiffrement de CAESAR considéré comme une addition modulo 26. Si les lettres de l'alphabet reçoivent les valeurs A=0,....Z=25, et qu'on appelle addition la combinaison d'une colonne et d'une ligne, le caractère se trouvant à l'intersection de la ligne et de la colonne est la somme, modulo 26.
Ici, 22 + 5 = 1 ,ce qui correspond à W + F = B

7.2.3.4. CHIFFREMENT DE VERNAM.

Consiste en une substitution polyalphabétique (voir chiffre de Vigenère) où la période de la clé est au moins aussi longue que le nombre de caractères du message à transformer.

Exemple : Le chiffrement de Vernam est celui qui fut appliqué initialement au texte de télécripteur. L'alphabet était en réalité le code Baudot et la clé était fournie par une boucle de bande perforée de façon quasi aléatoire.
Il consistait, en théorie, en une addition modulo 2, soit un OU exclusif entre les différents bits d'une clé en binaire et les caractères du texte clair en binaire également.

7.2.4. CHOIX DE LA CLE.

L'utilisation répétée de la clé ainsi que les possibilités de détection de celles-ci constituent les faiblesses de ces techniques. Si une clé était :

- aléatoire, (registre à décalages et génération de nombres au hasard),
- au moins aussi longue que le nombre de caractères du texte en clair à chiffrer,
- détruite après son utilisation pour un seul message,

le cryptogramme résultant serait indéchiffrable, même théoriquement.

Bien que le système à boucle perforée (Vernam) pourrait fournir des clés utilisées une seule fois, au fur et à mesure qu'augmente le volume du trafic des messages, la répétition devient une nécessité pratique. Autrement dit, la clé devient une boucle et le chiffre devient alors vulnérable.

Bien que les chiffres de Vigenère et de Vernam aient eu un grand intérêt pour les cryptologues au cours des années passées, Bryant Tuckerman (I) a montré qu'ils sont très vulnérables pour un analyste expérimenté faisant appel aux ressources de l'ordinateur.

Il est donc évident qu'il faut des méthodes beaucoup plus efficaces pour assurer la sécurité des données. L'utilisation du système de "chiffre bloc" permet d'éviter les inconvénients rencontrés dans les systèmes précédents.

7.2.5. SYSTEME DE CHIFFRE BLOC.

7.2.5.I. PRINCIPE DE FONCTIONNEMENT.

Cette transformation consiste à appliquer successivement la substitution et la transposition au texte original.

Note : - Dans la substitution : un caractère est remplacé par un autre.
- Dans la transposition : les caractères résultants sont soumis à une remise en ordre.

7.2.5.2. AVANTAGES.

L'amélioration de cette catégorie de chiffres et son adaptation à l'ordinateur dans lequel de nombreuses transformations successives et séries de transformations peuvent être exécutées rapidement et automatiquement ont entraîné une méthode de chiffrement à la fois très complexe mais souple permettant de traiter des groupes de données comme une unité. Cette dernière caractéristique est souhaitable car plus le bloc de données traité est long, plus le nombre de combinaisons par substitution et remise en ordre est élevé.

7.2.5.3. EXEMPLES D'APPLICATION.

I. Système de FEISTEL.

Les substitutions et transpositions sont exécutées en fonction d'un chiffre clé. L'important est que ces substitutions sont en réalité des transformations non linéaires, ce qui réduit le pouvoir cryptographique d'un décrypteur éventuel.

Pour donner une idée générale de la méthode, la Fig. $7.2.5.3_a$ décrit le traitement des I6 bits d'un sous-ensemble de l'ensemble du système. Les opérations et leur ordre d'exécution sont néanmoins représentatifs du système complet.

2. Système LUCIFER réalisé par SMITH (IBM Research)

Utilisant les principes de cryptologie mis au point par Feistel, ce dispositif chiffre (ou déchiffre) des messages de longueur quelconque par groupes de I6 octets (I28 bits) sous le contrôle d'une clé comportant I28 bits choisis arbitrairement. (Cette clé peut être fournie par une carte à piste magnétique.)
La Fig. $7.2.5.3_b$ illustre le principe du système de chiffrement.

Remarque : Chaque groupe de texte chiffré reçu est déchiffré de la même manière, en utilisant la clé ayant servi au chiffrement. (Toutes les transformations d'octets et toutes les additions modulo 2 sont répétées dans l'ordre inverse, en réalisant à l'envers les opérations réalisées pour le chiffrement.

(I) Voir à cet effet l'ouvrage de B. TUCKERMAN; "A Study of the Vigenère-Vernam Single and Multiple Loop Enciphering Systems"
IBM Report N° RC2879, Thomas J. Watson Research Center, Yorktown Heights, N.Y., I970.

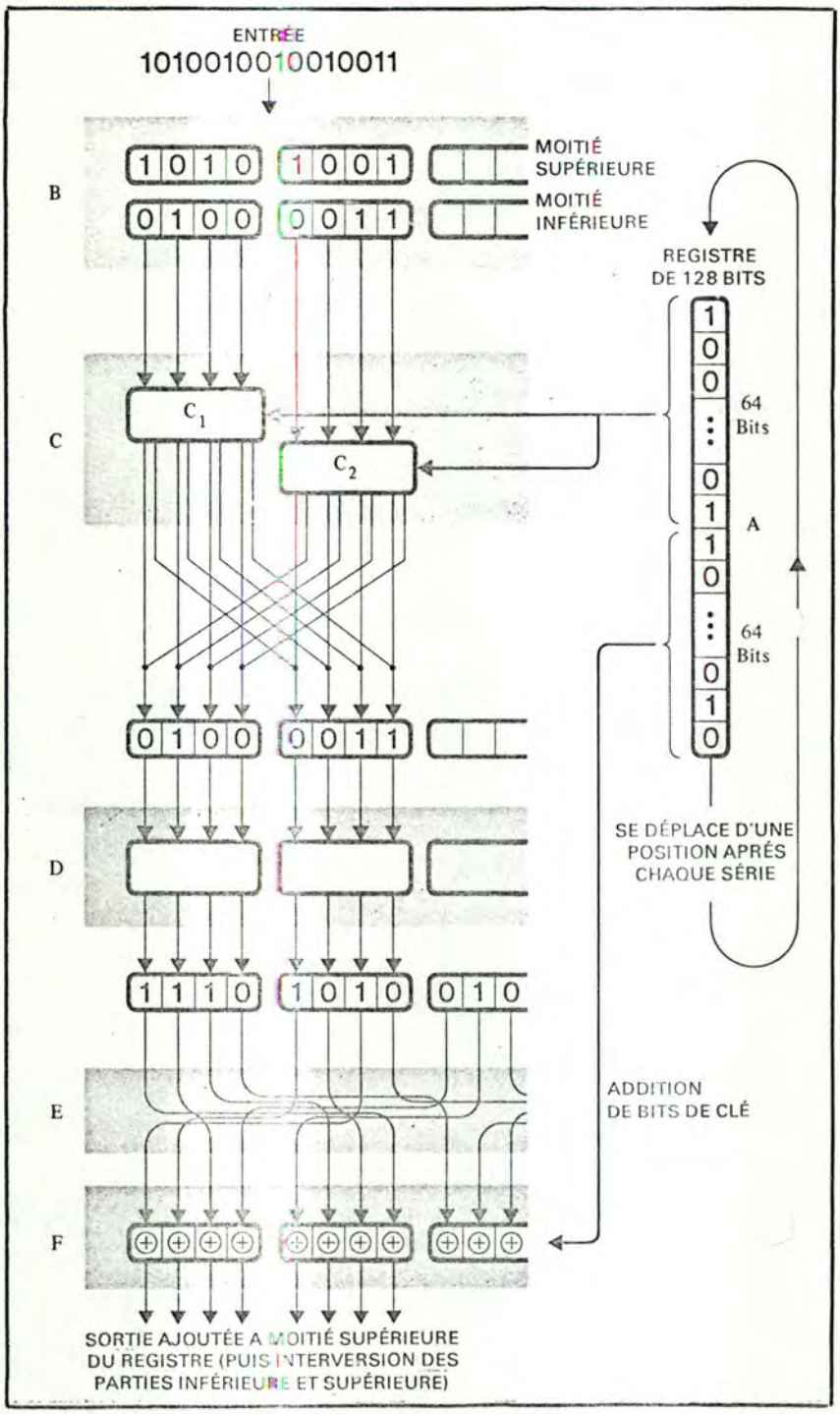


Fig. 7.2.5.3$_a$

Chiffrement de FEISTEL: Seuls I6 des I28 bits d'un seul bloc message sont représentés. Après introduction dans les parties inférieure et supérieure des registres de 2 bits (B), les blocs de 4 bits de la partie inférieure sont copiés et peuvent subir une transposition limitée en C, en fonction des valeurs des bits de la clé (en A).
En D, ces blocs sont alors soumis à des transformations non linéaires diverses. Les bits sont transposés séparément en E puis (en F) sont additionnés modulo 2 (signes + entourés) à d'autres bits de la clé. Ces sommes sont additionnées à la rangée supérieure des registres (B), et les contenus des moitiés inférieure et supérieure sont intervertis. La clé se déplace alors d'une position en vue de la série de chiffrement suivante.

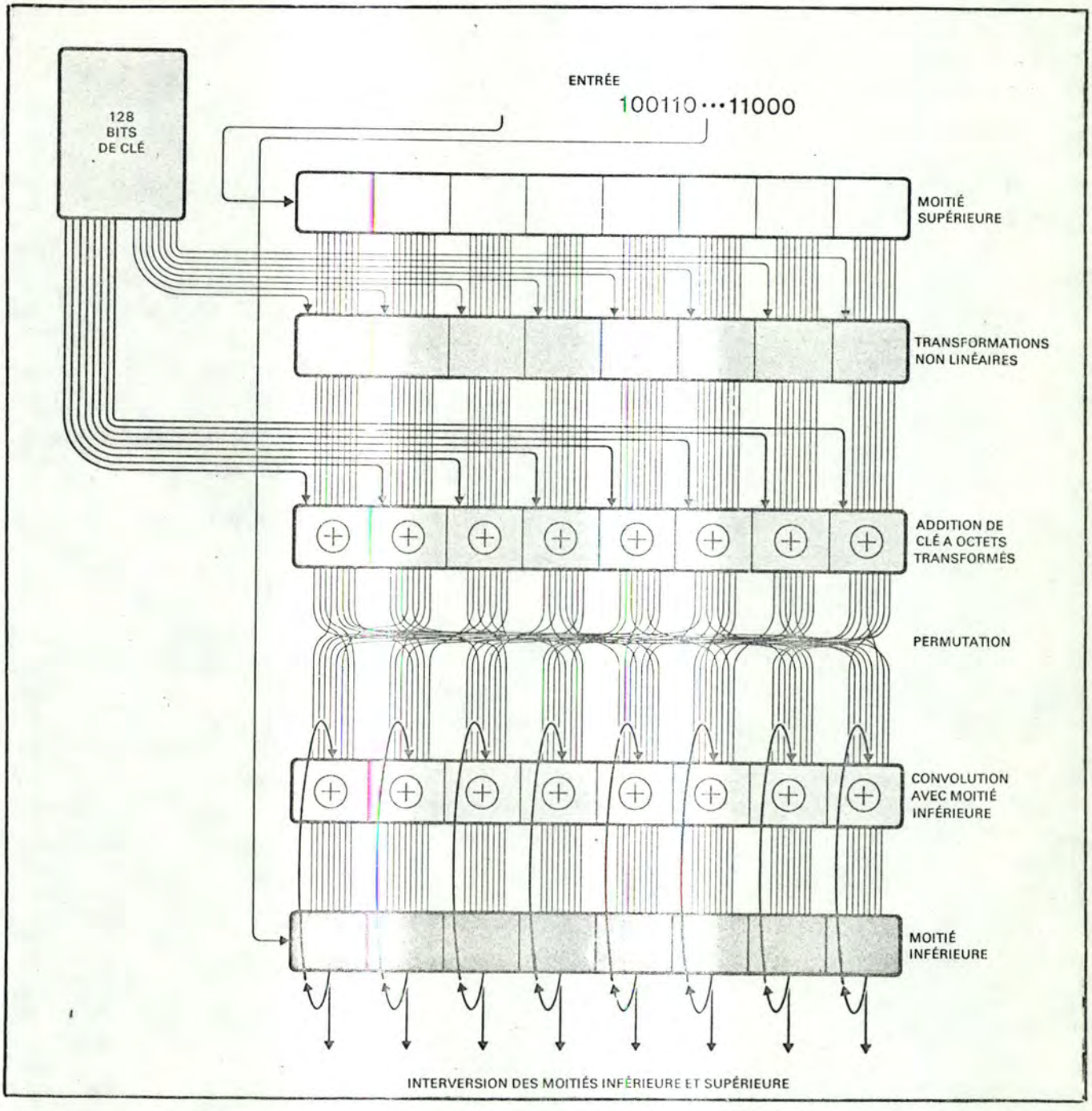


Schéma simplifié du chiffrement réalisé par le dispositif LUCIFER (procédure de chiffrement de FEISTEL modifiée par SMITH).
Un bloc de données de 16 octets (128 bits) est fractionné en parties inférieure et supérieure. Chacun des 8 octets de la moitié supérieure subit une transformation non-linéaire différente, sous le contrôle d'un bit de clé sélectionné, et à chaque octet ainsi transformé est ajouté un octet sélectionné de la clé.(Jusqu'ici, les octets conservent leur intégrité). Toutefois, pendant la permutation, les données sont décomposées en 64 bits redistribués et assemblés pour former de nouveaux octets, qui subissent une convolution par paire avec les octets de la partie inférieure du bloc de données.
Les parties inférieure et supérieure sont interverties: 16 séries alternées avec 15 interversions constituent le chiffrement complet d'un bloc de données.

fig. 7.2.5.3 b

7.3. DOMAINES D'APPLICATIONS.

Les techniques cryptographiques utilisées pour protéger les informations confidentielles, ont deux domaines d'application dans le cas des systèmes fonctionnant en télétraitement :

- le réseau de communication :
  - identification de l'utilisateur d'un terminal,
  - identification de l'ordinateur,
  - intégrité des messages (protection des données pendant la communication),
- les supports d'informations :
  - bases de données,
  - fichiers, (disques, tambours).

7.3.I. RESEAU DE COMMUNICATION.

7.3.I.I. INTRODUCTION.

Les méthodes qui suivent sont basées sur le fait que :

- chaque utilisateur possède une clé particulière,
- l'ordinateur possède un répertoire/dictionnaire complet de tous les utilisateurs autorisés et de leurs clés correspondantes.

7.3.2.I. IDENTIFICATION DE L'ORDINATEUR. (voir Fig. 7.3.I.2.)

La Fig. 7.3.I.2. illustre cette procédure :

- l'utilisateur donne son identité (A) en clair et transmet avec elle un segment de données arbitraires (X) composé d'une façon quelconque et chiffré avec sa propre clé. (I)
- l'ordinateur utilise la clé de A pour le déchiffrement, trouve la séquence de données arbitraires et lui annexe sa propre séquence arbitraire (Y) qu'il chiffre avec la clé de A, et renvoie à l'utilisateur A, ainsi que le segment (X). (2)
- lorsque le message est renvoyé, la concordance entre X "tel qu'envoyé" et X "tel que reçu" assure A de l'identité de l'ordinateur.

7.3.I.3. IDENTIFICATION DE L'UTILISATEUR.

I. En continuant la procédure décrite précédemment, la transmission ultérieure, en chiffre, de l'utilisateur A comprend le segment Y déchiffré ; si les deux versions de Y concordent, l'ordinateur s'est assuré à son tour de l'identité de l'utilisateur.

2. Dans une autre méthode, un mot de passe convenu, par exemple un nombre qui change de façon prévisible (voir section 5), peut être incorporé à un bloc de données et envoyé sous la protection d'un chiffre.
   Tout comme dans l'échange cité plus haut, la concordance totale entre segments d'identification repose sur l'utilisation de clés identiques.

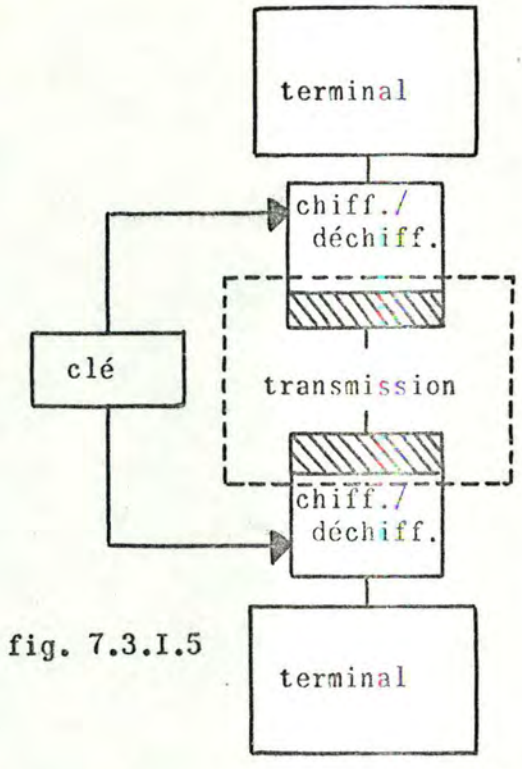


fig. 7.3.I.5

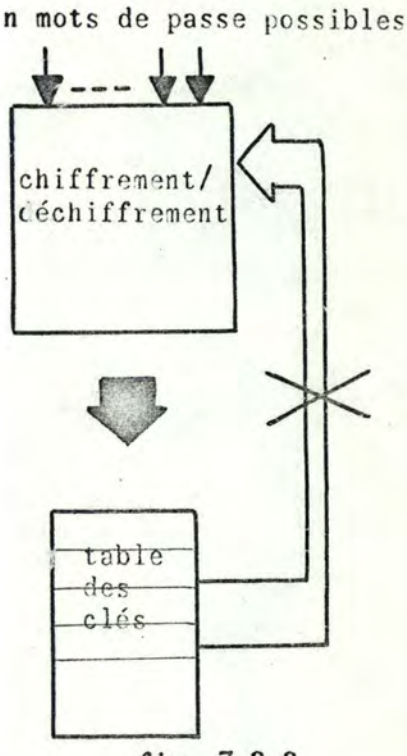


fig. 7.3.3

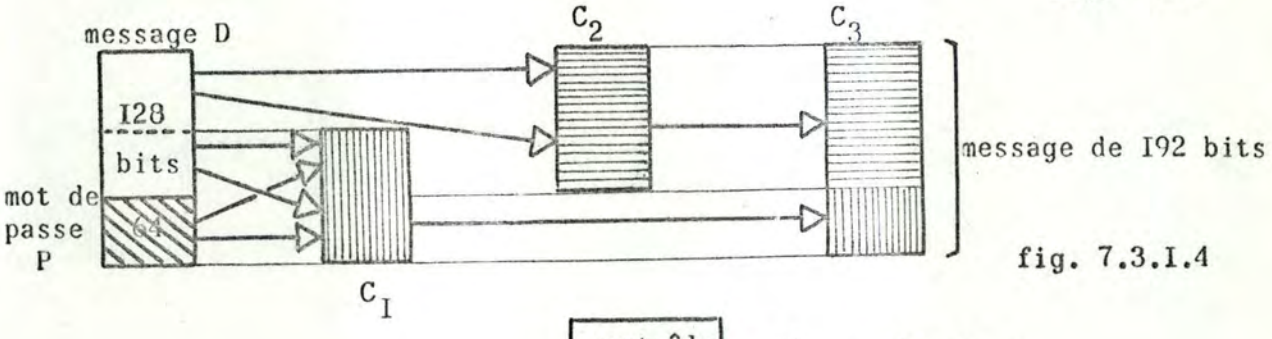


fig. 7.3.I.4

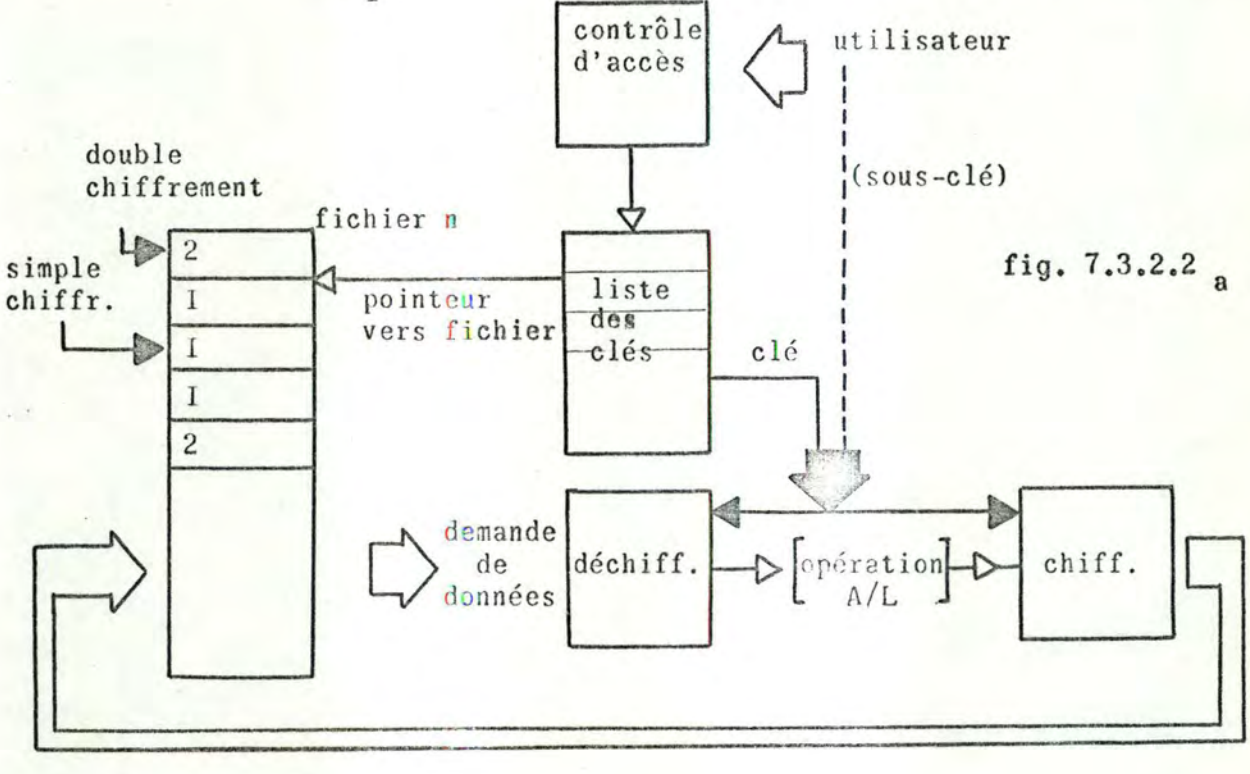


fig. 7.3.2.2 a

7.3.I.4. INTEGRITE DU MESSAGE : METHODE DE CHIFFREMENT PROGRESSIF.

Le chiffrement progressif, qui est un raffinement du système à chiffre bloc, (voir 7.2.5.) est illustré Fig. 7.3.I.4.

Dans ce système, un bloc chiffré CI est obtenu pour un mot de passe P et uniquement une partie d'un bloc de données D. Le chiffrement progresse alors d'un pas : le bloc C2 est obtenu pour une partie de CI et la partie restante de D.

Le chiffre effectivement transmis est C3 ; il est constitué d'une partie de CI et de l'entièreté de C2.

Côté réception, le déchiffrement doit s'éxécuter dans l'ordre inverse, jusqu'à ce que le mot de passe soit obtenu.

Remarque :L'ordinateur effectuera un contrôle complet du début à la fin de l'échange de messages. Un contrôle négatif résultant d'une erreur de transmission non détectée ou d'un incident provoque un brouillage complet de ce bloc de texte clair déchiffré, ce qui permet de faire la distinction avec une tentative de pénétration du système que pourrait faire un intrus habile, par exemple en introduisant des versions enregistrées de texte chiffré antérieur.

7.3.I.5. IMPLEMENTATION.

A. Au moyen d'une paire de dispositifs de chiffrement/dech.

PRINCIPE : Un dispositif hardware ("scrambler") placé à chaque extrémité de la ligne permet d'assurer les opérations de chiffrement/déchiffrement des données. Le chiffre obtenu (cryptogramme) dépend de la clé de l'utilisateur qui a actuellement (un à la fois) accès au système. La clé peut n'être utilisée qu'une fois. La zone de protection se situe entre les deux dispositifs. (Fig. 7.3.I.5)
La fonction utilisée pour le chiffrement doit pouvoir être inversée sinon le déchiffrement du message ne pourra être réalisé.

UTILISATION : Commutation de messages entre terminaux ou entre ordinateurs (terminaux intelligents).

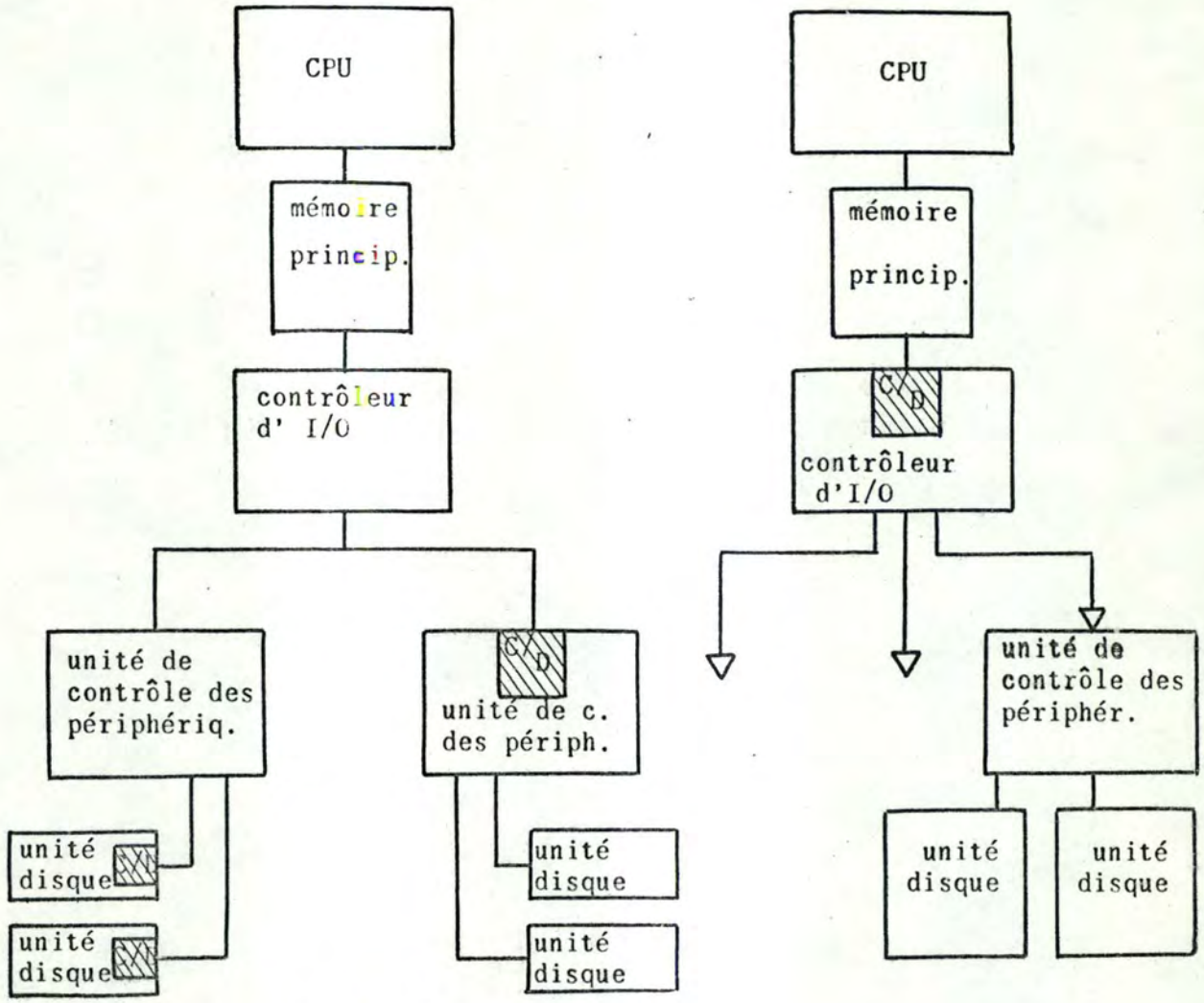
EXEMPLE : Dispositif "LUCIFER" (voir 7.2.5.3.)

B. Au moyen d'un multiplexeur FRONT- END.

PRINCIPE : Le multiplexeur permet la commutation automatique des clés de chiffrement/déchiffrement des différents utilisateurs d'un système télétraitement.
Il peut être essentiellement hardware ou comporter une partie software.
La complexité des circuits de ce dispositif est due au fait qu'il doit :

- assurer la commutation des clés et simultanément,
- se rappeler, pour chaque utilisateur, la position actuelle à l'intérieur de la fonction de transformation.

TRANSFORMATION: Systèmes de télétraitement où tous les utilisateurs utilisent simultanément la même fonction de transformation.



(a) fig. 7.3.2.4 (b) (c)

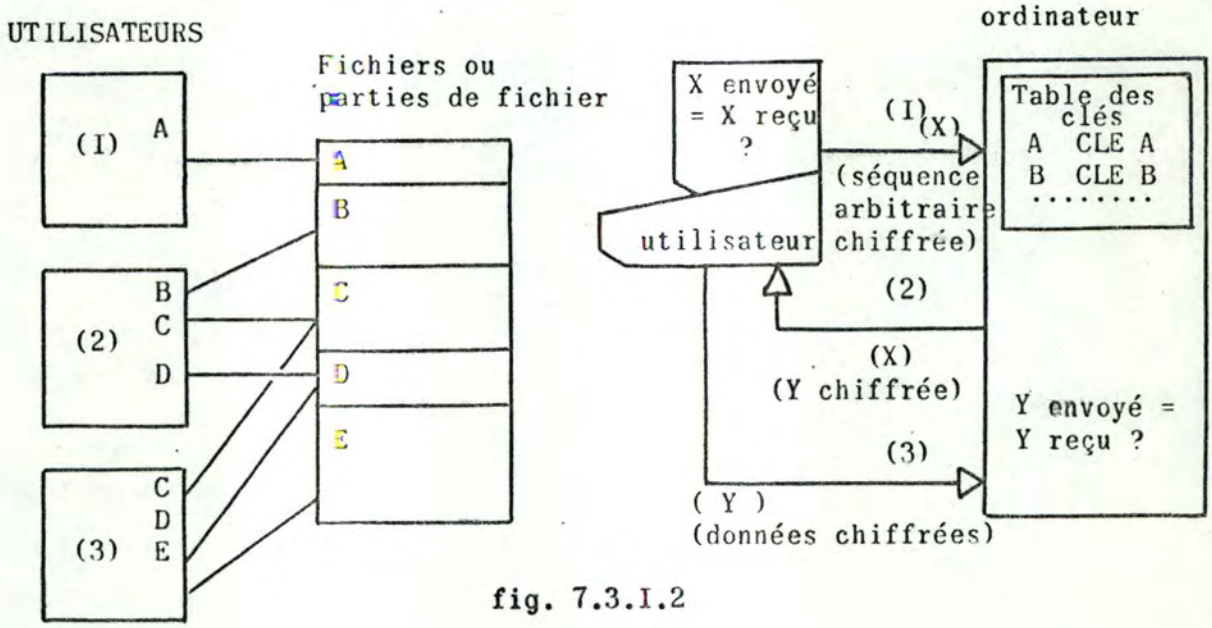


fig. 7.3.I.2

fig. 7.3.2.2 b

7.I.3.6. REMARQUE.

Les techniques cryptographiques peuvent être implémentées au moyen de dispositifs hardware, software ou utilisant les deux à la fois : les transformations software seront réalisées par le processeur central, les autres hardware seront implémentées dans les terminaux. Toutefois, le coût décroissant des dispositifs hardware (lié au coût des composants électroniques) a permis de coupler ceux-ci aux processeurs (ex.: Processeur central et processeur d'entrées/sorties).

7.3.2. SUPPORTS D'INFORMATIONS.

7. 3.2.I. INTRODUCTION.

Dans les systèmes fonctionnant en télétraitement, la clé, utilisée pour déchiffrer/chiffrer les données d'un fichier, doit être modifiée (mise à jour) soit :

- à chaque changement de programme (si le nouveau ne travaille pas sur le même fichier,
- chaque fois qu'un même programme change de fichier.

La solution immédiate est de stocker les clés dans une zone de mémoire protégée. (Ex. : système MULTIC) c'est-à-dire non-accessible aux utilisateurs.

7.3.2.2. CONTROLE DE L'ACCES AUX ENREGISTREMENTS D'UN FICHIER OU D'UNE BASE DE DONNEES.

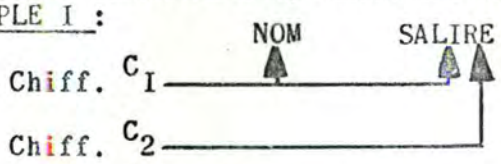
A. Une clé par fichier (ou par type d'enregistrement de la base de données.)

PRINCIPE : Les messages del'utilisateur sont soumis au système de contrôle d'accès. Si l'utilisateur est autorisé à accéder au fichier qu'il demande, une clé associée à un pointeur vers celui-ci sont obtenus à partir d'une table des clés.
La clé est passée à une procédure de de chiffrement/déchiffrement. (dispositif hardware ou routine software).

Les données seront déchiffrées avant leur traitement et rechiffrées si elles doivent être replacées dans le fichier (clé du fichier ou envoyées à un utilisateur.(clé de l'utilisateur.)
La Fig. 7.3.2.2. illustre la structure générale de ce système.

B. Plusieurs clés par fichier (ou par type d'enregistrement de la base de données.)

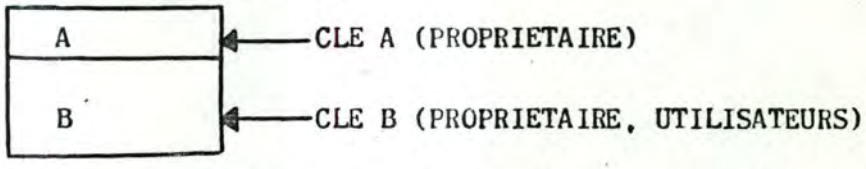
PRINCIPE : S'il est nécessaire de distinguer plusieurs niveaux de confidentialité entre les enregistrements d'un même fichier ou entre items d'un même enregistrement, on peut exécuter plusieurs chiffrements, (clés différentes) des données.
EXEMPLE I :



(double chiffrement)
- l'item"salaire" n'est accessible qu'aux util. possédant les 2 clés.

(autant de clés que de niveaux de confidentialité.)

EXEMPLE 2 : Le propriétaire d'un fichier qui désire partager une partie de son fichier avec d'autres utilisateurs peut la chiffrer à l'aide d'une clé différente du reste qui se retrouve ainsi automatiquement protégé.



Remarquons qu'on n'exécute plus les chiffrements sur les mêmes données (ex. I-item "salaire") mais sur des données différentes.

.que le propriétaire peut modifier la clé B s'il veut restreindre le nombre d'utilisateurs qui avaient précédemment accès à son fichier.

La procédure d'autorisation consiste à fournir à chaque utilisateur les clés des fichiers et parties de fichiers auquels il a accès. (voir Fig. 7.3.2.2. $_b$)

7.3.2.3. GENERATION DES CLES.

Partant du principe que l'existence de la table des clés en mémoire principale accroît la vulnérabilité du système, il sera préférable d'utiliser l'une des méthodes suivantes :

- stockage des clés dans une mémoire de type READ-ONLY ;
- génération au moyen d'un algorithme;
- assemblage de chaque clé à partir de sous-clés :
  - soit résidentes en mémoire,
  - soit partiellement résidentes (les parties non-résidentes sont alors fournies par l'utilisateur, par exemple, sous forme de préfixe ou suffixe à la sous-clé de la table) (voir Fig. 7.3.2.2. a)

7.3.2.4. IMPLEMENTATION.

Le dispositif de chiffrement/déchiffrement peut être implémenté à trois endroits différents :

- soit sur chaque armoire à disques : (Fig. 7.3.2.4. a)
  . cette implémentation présente l'avantage que toutes les informations (données, clés, identifiants) sont chiffrées ; ceci permet de protéger le disque en cas de vol.
  . elle requiert cependant de nombreux dispositifs.
- soit sur chaque unité de contrôle des périphériques :
  . seules les données sont chiffrées,
  . les zones de clés et d'identifiants (utilisées pour les opérations de recherche) ainsi que celles de contrôle (servant à la détection et à la correction des erreurs) ne peuvent être chiffrées puisque le déchiffrement n'est réalisé qu'à la sortie vers le contrôleur d'I/O. (Fig. 7.3.2.4. b).

- soit sur le contrôleur d'entrées-sorties : (Fig.7.3.2.4. c)

. le chiffrement/déchiffrement dépendra de la destination ou de la provenance des données : la procédure ne sera, par exemple, pas appliquée aux périphériques tels que l'imprimante, la console opérateur, le lecteur de carte.

7.3.2. DIFFERENCES ENTRE L'APPLICATION DES TECHNIQUES CRYPTOGRAPHIQUES AUX RESEAUX ET AUX SUPPORTS D'INFORMATIONS.

	RESEAUX	FICHIERS
I. CHIFFREMENT/ DECHIFFREMENT	Exécutés à deux endroits différents Deux copies de la clé	Exécutés au même endroit. Une seule copie de la clé.
2. FREQUENCE DE MODIFICATION	UNE ou PLUSIEURS session terminal, ou la durée d'un message. (La clé n'est jamais modifiée pendant la transmission d'un même message.)	--- (Théoriquement, la clé est la même pendant la vie du fichier.) (Pratiquement : . peut être changée de façon imprévisible. . entraîne alors, le recopiage du fichier ou l'archivage des clés précédentes.
3. DUREE DE VIE D'UNE INFORMATION CHIFFREE.	Très courte : le déchiffrement commence avant la fin du chiffrement.	Dépend de la fréquence de mise à jour du fichier.
4. CARACTERES DE CONTROLE.	. sont envoyés avec le message, : ne sont pas chiffrés.	---
5. NOMBRE DE PERSONNES CONCERNEES.	I seul utilisateur par communication.	Plusieurs utilisateurs (éventuellement avec des niveaux de confidentialités ≠) par fichier.

7.3.3. CONCLUSIONS.

La protection offerte par les techniques cryptographiques n'est pas théoriquement invulnérable (sauf dans la technique utilisée par MULTICS- voir Fig. 7.3.3.) bien que les problèmes qu'aurait à résoudre un décrypteur éventuel semblent difficilement surmontables, compte tenu du temps nécessaire et des coûts que cela entraînerait.

En les associant à d'autres mécanismes de protection (voir sections précédentes), on peut obtenir un degré de sécurité élevé ; toutefois, ces techniques sont les seules qui permettent de réaliser la protection des données pendant leur transmission ou durant leur stockage sur un support. (protection contre le vol, l'impression ou la copie (sans passer par le système d'exploitation) sur un autre support.

section 8 : contrôle et maintenance des fonctions d'identification et d'autorisation : le responsable de la sécurité.

8.I. AVANT-PROPOS.

Afin de décourager toute tentative de violation du système de sécurité de la part de personnes non-autorisées, il est nécessaire de lui adjoindre une fonction de contrôle et de maintenance.

Afin de pouvoir situer le rôle de celle-ci dans le cas d'un système de sécurité appliqué aux ordinateurs fonctionnant en télétraitement (fonctions d'identification et d'autorisation), nous allons faire apparaître les différents niveaux de gestion qui participent à la définition, la conception, l'implémentation et la maintenance d'un système de sécurité.

8.2. METHODOLOGIE DE LA MISE EN PLACE DU SYSTEME DE SECURITE.

Les différents aspects d'un système de sécurité seront pris en compte par trois niveaux de gestion :

- la direction générale,
- la gestion centrale,
- la gestion des opérations.

Chacun de ces niveaux contribue à la réalisation et à l'efficacité du système de sécurité. La Fig. 8.2. permet d'illustrer ces différents niveaux de gestion.

8.2.I. OBJECTIF DE LA DIRECTION GENERALE.

Pour chaque application, celle-ci s'attachera à établir les politiques permettant de protéger, contre tout préjudice, des données confidentielles ou vitales pour l'entreprise, stockées et traitées par le centre informatique.

Rappelons qu'un préjudice résulte d'une ou de plusieurs activités non-autorisées suivantes :

- observation (n'affecte pas les données),
- extraction (retrait ou copie des données),
- altération (modification des données ou d'une procédure),
- addition (insertion de données étrangères),
- utilisation (usage des ressources hardware ou software du système)?

La détermination de la nature et de l'étendue des dispositifs de protection nécessaires peut être réalisée sur base d'un compromis entre quatre facteurs interdépendants.

8.2.I.I. FACTEURS PERMETTANT D'ESTIMER LA NATURE ET L'ETENDUE DES DISPOSITIFS DE PROTECTION REQUIS.

I. Le but de l'application,
2. La configuration nécessaire : (batch, télétraitement...)
3. Le degré de confidentialité requis : (éviter toutes modifications par une personne non-autorisée à accéder à la base.)
4. Coûts supplémentaires :

   . en hardware (équipement supplémentaire : serrures, dispositifs d'effacement ou d'inhibition d'empression des mots de passe),

   . en software (overhead + coût dû aux procédures d'identification, d'autorisation, de contrôle et de maintenance.)

   . coût, pour intrus, d'acquisition ou de modification des données,

   . coût, pour le propriétaire, de remplacement d'une donnée détruite ou modifiée.

8.2.I.2. ANALYSE DE COUTS.

L'étude d'opportunité permettant de dégager les politiques de protection des données confidentielles de l'entreprise comportera donc une analyse de coûts.
La Fig. 8.2.I.2. permet d'illustrer le résultat de cette analyse. Partant du degré de sécurité correspondant au minimum de la courbe du coût total, on constate qu'une augmentation sensible du degré de sécurité entraîne un accroissement considérable du coût des mesures de sécurité supplémentaires.

Remarques:

. Le but d'un système de sécurité est de réduire la probabilité d'avoir un préjudice, à un niveau acceptable (le plus bas possible), et d'assurer un rétablissement adéquat lorsqu'un préjudice se produit. Nous n'exigerons pas d'avoir une sécurité totale : IOO % de sécurité ne résulterait pas d'un système utilisable vu la complexité, le coût et l'overhead important qu'il entraînerait .

. Aucune règle ne peut être utilisée pour examiner la relation coût-efficacité de mesures de sécurité : même dans des situations où tous les facteurs significatifs (voir plus haut) peuvent être déterminés, des facteurs subjectifs tels que la loyauté du personnel, (difficilement quantifiable) peuvent exercer une grande influence sur l'efficacité du système de sécurité mis en place.

. L'analyse de coûts est propre à chaque entreprise, ce qui sous-entend qu'un système de sécurité en informatique dépend de l'entreprise où il est implanté.

8.2.2. OBJECTIF DE LA GESTION CENTRALE. (ou NIVEAU CENTRAL DE GESTION).

La gestion centrale s'attachera à concevoir le système de sécurité. Elle sera assurée par une équipe de spécialistes.

Cette tâche de conception peut être subdivisée en deux sous-tâches :

. conception et programmation de contrôles précis et élaborés des accès aux données confidentielles.

. association de ces contrôles avec les mesures prises par la gestion des opérations (interdépendance entre la gestion centrale et la gestion des opérations.)

8.2.2.1. FACTEURS INFLUENCANT LA CONCEPTION DU SYSTEME DE SECURITE.

1. L'environnement du système,
   (ex. : batch, télétraitement ou les deux à la fois.)
2. Réseau de communications,
   (ex. : lignes locales, privées, louées ou commutées).
3. La valeur des informations stockées,
   (ex. : données nécessitant des précautions spéciales),
4. Ressources système,
   (ex. : le système d'exploitation peut fournir des supports de test et admet la résolution de problèmes en mode interactif.)

8.2.2.2. OUTILS DE CONCEPTION.

(voir sections 1 à 7 du présent chapitre).

8.2.2.3. OUTILS D'AIDE A LA MISE AU POINT.

Les outils d'aide à la mise au point constituent un ensemble de phases de contrôle ou de vérification.

Dans le cas des systèmes d'ordinateurs fonctionnant en télétraitement, nous pouvons considérer :

- d'une part, une phase de mise au point ou de révision (auditing) des programmes; celle-ci concerne :
  . les programmes d'application,
  . les utilitaires et programmes d'aide à la mise au point (routines de tracing, de display...),
  . les routines de sécurité (fonctions d'identification et d'autorisation, langage de mise à jour des tables de sécurité ;)
- et d'autre part, une phase de vérification ou de contrôle du déroulement :
  . des procédures d'identification et d'autorisation,
  . de la procédure de maintenance des tables de sécurité (tables de mots de passe, tables d'autorisations).

A. Phase de mise au point ou de révision des programmes : l'AUDIT en informatique, ses difficultés, ses solutions.

La révision, la vérification ou la mise au point d'un programme d'ordinateur pose un certain nombre de problèmes particuliers spécifiques aux techniques informatiques ;

I. Les supports d'information ne sont pas lisibles par l'homme :

. Pour effectuer des contrôles sur de telles informations non directement accessibles, on sera obligé de réaliser et d'utiliser des programmes spéciaux permettant de les faire apparaître (utilitaires) sur papier, en totalité, par échantillons, en comparaison ou par exception.

2. Les méthodes et règles de traitement sont appliquées par des programmes :

. Il est donc nécessaire d'entrer dans des programmes pour évaluer et vérifier la fiabilité de ces méthodes et de ces règles. Il sera souvent très difficile de vérifier si les règles élémentaires de sécurité ont été suivies. Il est donc nécessaire d'insérer des dispositifs de protection et de contrôle au niveau, soit du système de gestion de la base de données (comme le préconise CODASYL - voir rapport du DBTG), soit au niveau des routines d'accès du système d'exploitation.

3. Les programmes sont exploités par des ordinateurs :

. A ce stade, les fraudes et les erreurs sont donc encore possibles, même avec des programmes présentant un haut degré de sécurité. Il y aura donc lieu d'auditer également les procédures d'exploitation, en particulier sous l'aspect de l'impossibilité de passer outre aux contrôles programmés et sous celui des risques de pertes d'informations en cas de reprise après arrêt imprévu.

. Exemple : L'information transmise depuis le dernier point de contrôle est perdue totalement ou partiellement sans que l'on sache très bien jusqu'où car l'asynchronisme des opérations rend difficile la description du système au moment de la défaillance.

4. Les applications doivent être maintenues en permanence :

. Une application auditée hier risque de ne plus être valable le lendemain (du point de vue sécurité) à la suite d'opérations de maintenance. Comme il semble exclu d'en refaire l'audit systématiquement après chaque maintenance, il faudra s'assurer qu'il existe des normes très précises de modification des programmes, comportant entre autres des autorisations et attestations signées par le responsable de la sécurité du système.

Afin de faciliter cette révision et mise au point, il sera nécessaire de prévenir le responsable de la sécurité lors de tentatives d'accès non-autorisées et de tenir à jour des fichiers où seront enregistrées toutes les tentatives de violation du système de sécurité et toutes les modifications des tables de sécurité.

B. Phase de contrôle du déroulement des procédures du système de sécurité.

Cette phase de contrôle peut se subdiviser en trois étapes :

- une étape d'enregistrement, sur un fichier "mouvements", des activités non-autorisées des utilisateurs ;
- une étape d'analyse de ces activités ;
- une étape d'intervention permettant d'inhiber tout accès aux programmes, données et tables de sécurité.

La Fig. 8.2.2.3. permet d'illustrer les différentes étapes d'une phase de contrôle. Nous allons examiner celles-ci dans le cas du contrôle du déroulement des procédures du système de sécurité.

I. Contrôle du déroulement des procédures d'identification et d'autorisation.

Etape 1 : Enregistrement de toutes les tentatives (accidentelles ou intentionnelles) de violation du système de sécurité.

Exemple de tentative de violation :

- mot de passe incorrect,
- identification invalide du terminal,
- demande de données non-autorisées.

Etape 2 : Intervention immédiate / celle-ci consiste à prendre certaines mesures dans le but d'éviter toute tentative ultérieure.

Exemple d'intervention immédiate :

- lors de la première tentative :
  . enregistrement;
- lors de la seconde tentative (en provenance du même terminal et au cours d'une même session) :
  . enregistrement,
  . interruption (arrêt) du job de l'utilisateur,
  . blocage du terminal pendant un certain laps de temps,
  . avertissement au responsable local de la sécurité.
- Note : La remise en route du terminal nécessitera l'intervention de ce responsable.

Etape 3 : Analyse journalière et hebdomadaire de la liste des tentatives de violation afin de déterminer les activités non-autorisées.

Exemple :

Un nombre élevé de tentatives peut mettre en évidence le fait qu'un utilisateur expérimente le dispositif de protection. Exemple : succession de mots de passe incorrects.
Par contre, un nombre anormalement faible de tentatives peut signifier que les utilisateurs ont trouvé le moyen d'outrepasser les routines de sécurité ou d'enregistrement des violations.

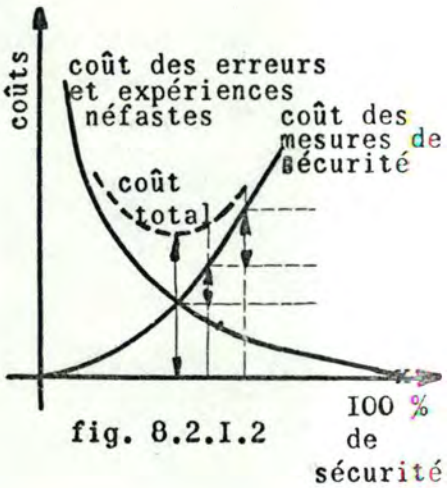


fig. 8.2.I.2

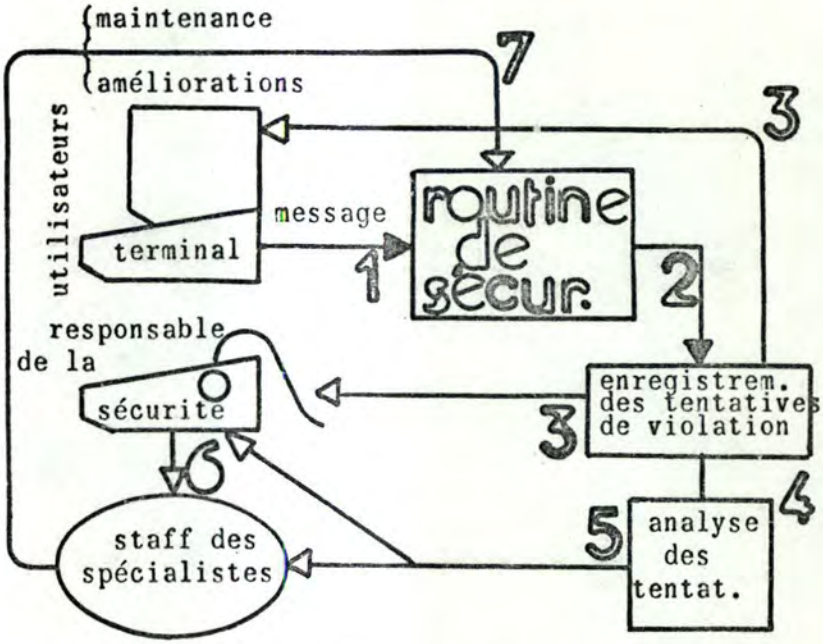


fig. 8.2.2.3$_a$

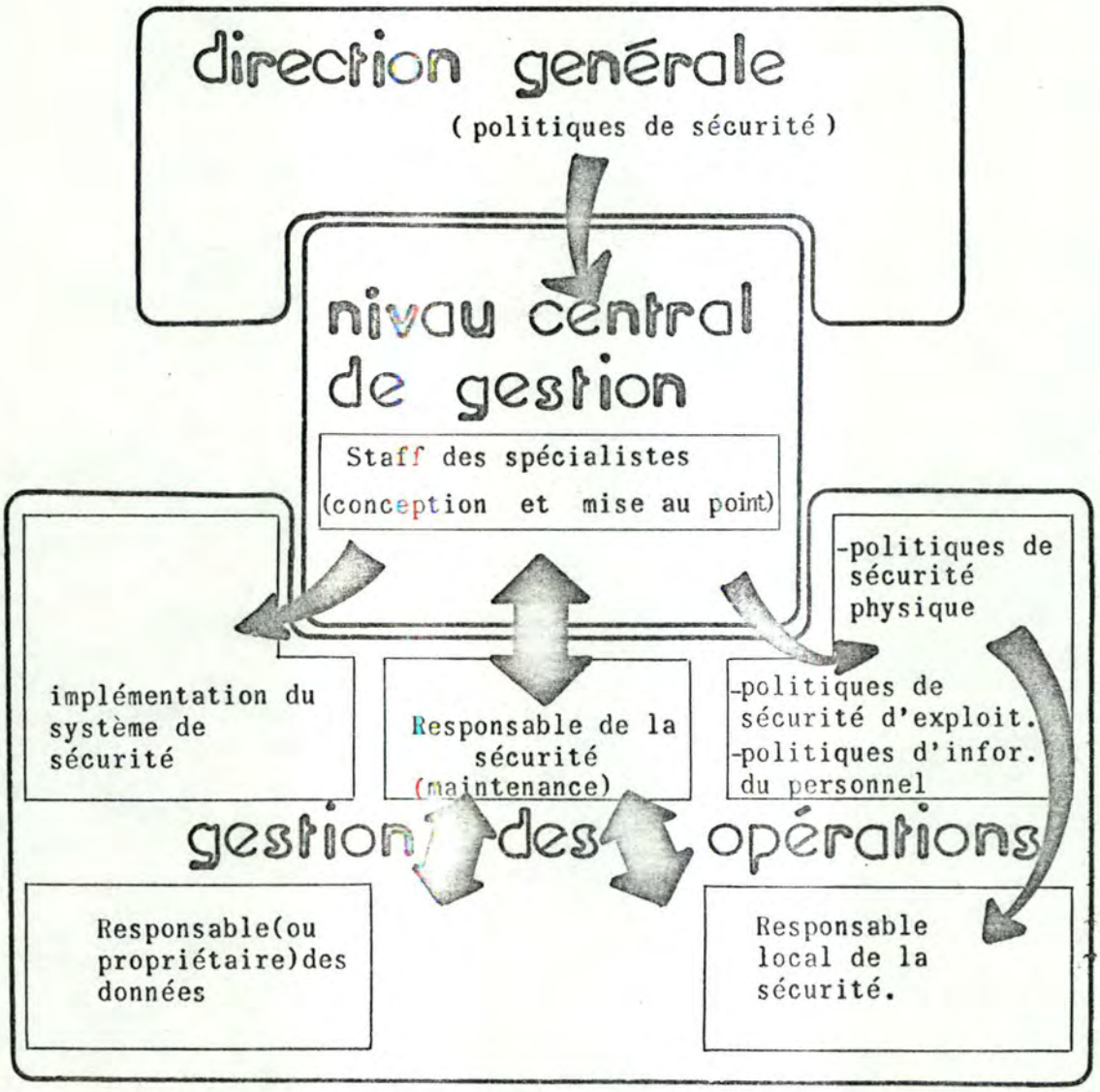


fig. 8.2

Cette étape d'analyse peut être éventuellement suivie d'une étape d'intervention qu'on pourrait qualifier de "différée" afin de la distinguer de l'étape 2. Elle consistera par exemple à modifier l'ensemble des mots de passe.

2. Contrôle du déroulement de la procédure de maintenance des tables de sécurité.

Nous avons vu précédemment que toute personne capable de modifier les tables de sécurité peut théoriquement et pratiquement avoir accès à la totalité du système. Ces tables devront donc être protégées efficacement. Les étapes de la phase de contrôle, quoique sensiblement les mêmes que précédemment, seront néanmoins plus rigoureuses.

8.2.3. OBJECTIFS DE LA GESTION DES OPERATIONS.

La gestion des opérations assurera l'implémentation et la maintenance du système de sécurité. De plus, elle s'efforcera d'améliorer celui-ci en promouvant des politiques de sécurité physique (accès à la salle ordinateur, aux librairies...) de sécurité d'exploitation et d'information du personnel.

Après avoir dégagé une méthodologie de la mise en place d'un système de sécurité des données appliqué aux systèmes de télétraitement, nous allons nous intéresser aux personnes responsables du contrôle et de la maintenance de ce système.

Pratiquement, la gestion des opérations est étroitement liée au niveau central de gestion (voir Fig. 8.2.)

Note : d'une part : nous ne développerons pas, dans le cadre de cette étude, la partie concernant les politiques de sécurité physique, de sécurité d'exploitation et d'information du personnel ; ces politiques seront toujours définies, quel que soit le but du programme de sécurité.

d'autre part : un exemple d'implémentation sera présenté au chapitre IV.

8.2.3.I. ZONES ET PERSONNES RESPONSABLES DE LA SECURITE.

Dans le cadre d'un système fonctionnant en télétraitement, les responsabilités de contrôle et de maintenance à assumer peuvent être réparties sur trois zones :

- l'installation de l'ordinateur (endroit où se situe l'ordinateur),
- le propriétaire des données,
- l'endroit où se situe le terminal et son utilisateur.

Chacune de ces trois zones est donc responsable de la sécurité. Toutefois, la direction de l'installation de l'ordinateur a les responsabilités fondamentales suivantes :

. établir des procédures standarts de contrôle, (en accord avec le propriétaire des données et les endroits où sont disposés les terminaux.

. être le point central des communications entre les utilisateurs et les propriétaires des données.

. être au courant des procédures de sécurité locales (endroits où se situent les terminaux).

Les responsabilités de contrôle et de maintenance du système de sécurité seront assumées :

. au niveau de l'installation de l'ordinateur par une seule personne : le responsable de la sécurité (security officer) ;

. localement : par un responsable local de la sécurité : (local security officer) ;

. par le propriétaire des données.

A. Rôle du responsable de la sécurité.

Il doit assumer au jour le jour le rôle d'administrateur et de superviseur de la sécurité, en fonction des directives fournies par les spécialistes qui ont conçu le système de sécurité (niveau central de gestion).

Ce rôle d'administrateur et de superviseur consiste :

. à contrôler le déroulement des procédures d'identification et d'autorisation, et à prendre des actions en cas de tentatives de violation répétées :

Exemple : . examen du fichier contenant les enregistrements de toutes les tentatives de violation des procédures de sécurité (voir 8.2.2.3.) ;

. examen des listings console et des états statistiques décrivant l'activité du système.

. à assurer la maintenance du système de sécurité :

Exemple : . il sera le seul à pouvoir accéder aux tables de sécurité (tables des mots de passe, des clés, des autorisations) et donc à les modifier (modification des mots de passe, mise à jour des tables d'autorisations).

(le propriétaire des données sera chargé de lui fournir les règles d'accès à ses données ainsi que les noms des personnes auxquelles il accorde l'autorisation d'y accéder).

. à estimer l'efficacité du système de sécurité et à revoir la conception du système de sécurité avec l'équipe des spécialistes (voir phase d'analyse en 8.2.2.3.)

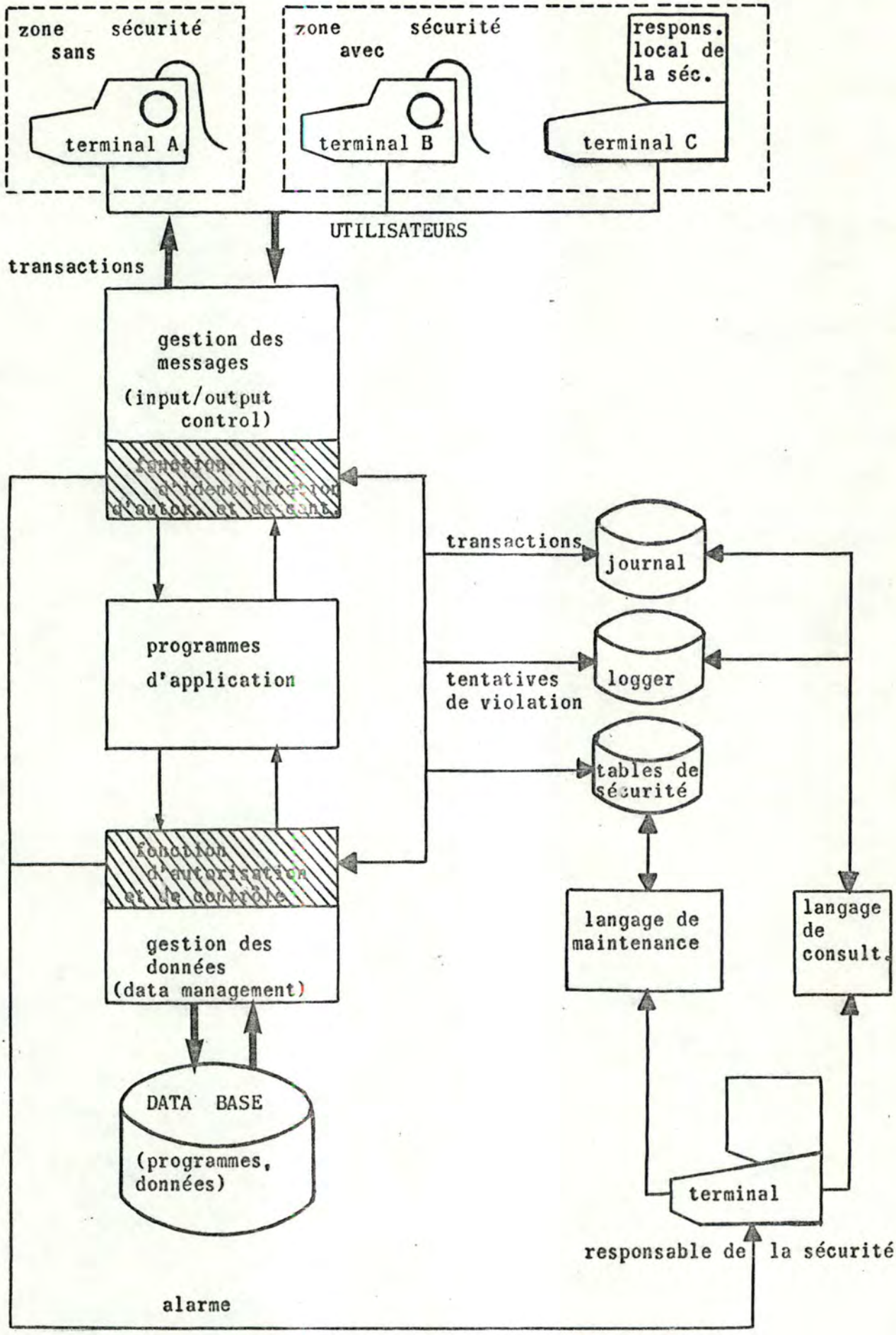

zone sécurité sans
terminal A
zone sécurité avec
terminal B
respons. local de la séc.
terminal C
UTILISATEURS
transactions
gestion des messages (input/output control)
fonction d'identification d'autor. et de cont.
transactions
journal
programmes d'application
tentatives de violation
logger
tables de sécurité
fonction d'autorisation et de contrôle
gestion des données (data management)
langage de maintenance
langage de consult.
DATA BASE
(programmes, données)
terminal
responsable de la sécurité
alarme

fig. 8.2.2.3$_b$

B. Rôle du responsable local de la sécurité.

Chaque zone (ex. : filiales d'une société) ou local (ex. : services d'une entreprise) où sont implantés des terminaux doit désigner un responsable de la sécurité (ex. : le chef du service ou du département). Celui-ci recevra des directives du responsable de la sécurité au niveau de l'installation.

Son rôle consistera principalement :

. à assurer la protection du local ou des terminaux (voir section 2) s'ils sont destinés à l'entrée d'informations (programmes, données) confidentielles ;

. à s'assurer que les utilisateurs respectent les directives de sécurité :

Exemple : - baisser la luminosité des caractères visualisés sur un terminal à écran cathodique lors de l'introduction du mot de passe ou de données confidentielles ;

- vidage des informations contenues dans les buffers, à la fin d'une session terminal ;

. à débloquer les terminaux bloqués par le système de sécurité à la suite de deux tentatives de violation successives.

(Le responsable de la sécurité de l'installation lui enverra périodiquement la liste de toutes les tentatives perpétrées à partir de son local ou de sa zone).

C. Rôle du propriétaire des données. (FILE OWNER)

En plus du responsable local de la sécurité, on peut désigner un responsable pour chaque fichier de la base.
Il fournira au responsable de la sécurité de l'installation la liste des personnes autorisées à accéder à ses données ainsi que les règles d'autorisation qui permettront de mettre à jour les tables de sécurité.

8.2.3.2. REMARQUE : LEGISLATION CONCERNANT LES BASES DE DONNEES RELATIVES AUX PERSONNES PHYSIQUES OU MORALES.

Actuellement, les bases de données relevant du secteur public ou du secteur privé, relatives aux personnes physiques ou morales, et contenant le nom, la raison sociale ou la dénomination, le numéro personnel ou toute autre indication susceptible d'identifier la personne sont soumises à une législation spécifique. Celle-ci vise à assurer la protection des libertés individuelles menacées par la détention et l'utilisation abusives de données sur les personnes.

Dans le cadre européen, seule, la Suède a mis en vigueur une loi abordant l'intégralité du problème mais partout des projets de loi (Ex. : Belgique, France, U.S.A.) ont vu le jour, des commissions d'experts et de juristes ont été constituées.

De l'ensemble de ces études, il ressort clairement qu'il faut :

- mettre sur pied une législation spécifique. Les propositions des projets de loi sont, en général , les suivantes :

  1. Interdire toute collecte de données concernant la religion, la race, l'appartenance syndicale ou politique, la vie privée, le secret des personnes morales, les sanctions amnistiées....
  2. Chacun doit avoir connaissance de ce qui est enregistré sur lui et pouvoir obtenir facilement des rectifications.
  3. Nécessité d'une autorisation spéciale et préalable pour toute communication entre fichiers.
  4. Obligation de déclarer certains fichiers privés.
  5. Nécessité de créer un "Haut Comité" chargé du contrôle et de l'adaptation permanente des mesures réglementaires.

  Exemple : (Voir annexe D : projet de loi belge sur les fichiers de personnes - extrait de OI-HEBDO n° 313 du 16 décembre 74)

  Bien qu'il soit plus complet que la majorité des projets actuels, il concerne (comme tous les autres) les bases données et non les fichiers.

- Nécessité d'une déontologie des informaticiens.

  Celle-ci porte principalement sur :

  . le respect de la loi,
  . le respect de l'information pour tous ceux qui collaborent au traitement des données.

  Exemple : (voir annexe C. : la déontologie des informaticiens des administrations publiques -)

- Necessité de mettre au point des moyens de protection technologiques (hardware et software).
  Exemple : (voir sections 2 à 7 du présent chapitre).

En examinant en détail les projets de loi et les codes de déontologie actuels, on constate qu'ils s'attachent à réaliser un difficile équilibre : assurer une protection efficace des libertés individuelles sans entraver le développement de l'informatique. Jusqu'à présent, ils n'y sont pas parvenus.
(voir, par exemple, l'article 17 du projet de loi belge).

CHAPITRE 3:
élaboration d'un programme de contrôle d'accès (niveau central de gestion)

section 1: phase de conception des fonctions d'identification, d'autorisation et de contrôle.

I.I. AVANT-PROPOS.

En suivant la méthodologie développée précédemment, nous allons concevoir un programme de contrôle d'accès à une base de données à partir de terminaux éloignés. Il s'agit donc de concevoir une fonction d'identification, une fonction d'autorisation et une fonction de contrôle des deux précédentes.

Parmi l'ensemble des techniques décrites au chapitre 2, nous avons fixé notre choix sur une technique software, tant pour l'identification que pour l'autorisation. La fonction de contrôle sera donc essentiellement software. Les techniques retenues sont les suivantes:

Fonction d'identification :

Seule l'identification du terminal sera prise en considération. Elle sera basée sur la technique des mots de passe. (voir implémentation : output CSMAIN)

Fonction d'autorisation :

Utilisation de la technique des tables d'autorisations : trois tables permettront d'assurer le contrôle de l'accès aux programmes, fichiers et données. (voir Fig. I.I.)

I.2. STRUCTURE DES TABLES D'AUTORISATIONS

I.2.I. TABLE I : TABLE DES UTILISATEURS.

La première entrée est réservée au langage de maintenance et porte le numéro d'identification I, le nombre d'entrées actuellement remplies dans la table, une table(de bits)des groupes existants (ayant une entrée dans la table des groupes), une partie non-utilisée remplie de zéros.

Les entrées suivantes comportent 4 items :

item I : numéro d'identification de l'utilisateur,
item 2 : sa clé ou son mot de passe,
item 3 : groupe auquel il appartient,
item 4 : sa responsabilité ou sa fonction.

Le numéro de groupe indique l'entrée correspondante dans la table des groupes.

Remarque : La table des utilisateurs contient une entrée par utilisateur. Celui-ci peut être une seule personne (clé individuelle) ou un ensemble de personnes (département ou entreprise). Dans ce dernier cas, toutes ces personnes ont une clé commune (voir avantages et inconvénients au chapitre 2). En regroupant par exemple les utilisateurs par département, on peut donc réduire considérablement la table des utilisateurs.

I.2.2. TABLE 2 : TABLE DES GROUPES.

Cette table va nous permettre de regrouper les utilisateurs ayant les mêmes privilèges. Toutefois, au sein d'un même groupe, chaque utilisateur a sa propre clé d'accès (par la table des utilisateurs); donc, bien qu'ils soient regroupés, la fonction d'identification peut identifier un utilisateur.

Comme précédemment, ce dernier peut être une seule personne (personne physique) ou un ensemble de personnes (personne morale). Un groupe est alors constitué de tous les départements ou entreprises ayant accès aux mêmes programmes, fichiers et données.

La table des groupes comprend une entrée par groupe, plus une entrée utilisée par les routines du langage de maintenance de la table.

Celle-ci comprend trois tables de bits et trois zones de type "compteur" :

a) table des groupes (bit 0 : groupe inexistant),
(bit 1 : groupe présent).

b) table des programmes (conventions identiques).

c) table des fichiers (idem).

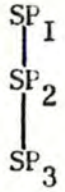
Chaque entrée correspondant à un groupe comporte :

- un item par programme d'application : le code partie-programme (CPP) servira au moniteur de chaque programme d'application afin de rendre accessible à l'utilisateur certaines parties de ce dernier.

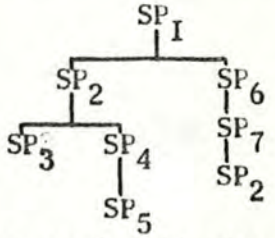
Une partie de programme désigne soit :
- le programme d'application tout entier,
- plusieurs de ses sous-programmes ou un seul,
- une ou plusieurs instructions à l'intérieur d'un sous-programme.

Les sous-programmes seront hiérarchisés suivant l'une des deux structures suivantes :

STRUCTURE LINEAIRE



STRUCTURE ARBORESCENTE



Chaque sous-programme portera un numéro d'ordre dans la hiérarchie.

- deux items par fichier :(I6 fichiers maximum)
  - . item I : code enregistrement (CE) permettant d'indiquer les enregistrements du fichier accessibles à ce groupe.
  - . item 2 : code masque (numéro du masque à utiliser pour ce fichier et pour ce groupe d'utilisateurs).

Remarques:concernant le code partie-programme et le code enregistrement:

Un groupe aura accès :

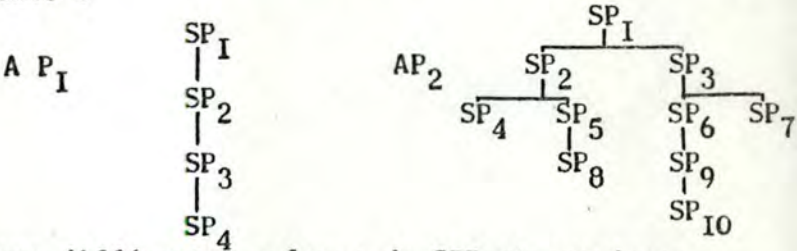
a) à un programme d'application si le CPP correspondant à ce programme est différent de 0 ;

b) à un fichier si les CE et CM correspondant à ce fichier sont différents de 0 ;

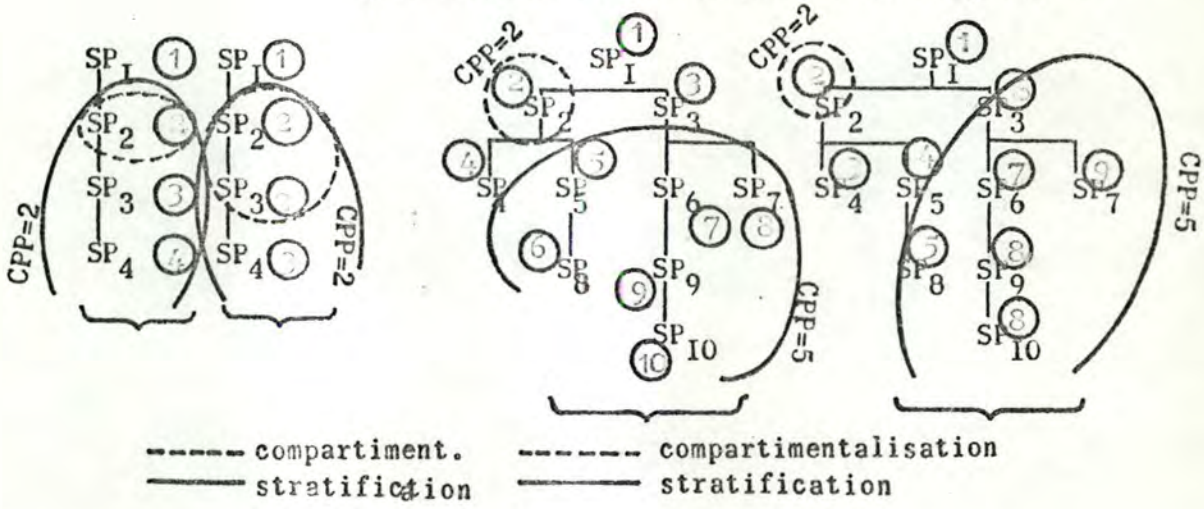
c) à un seul sous-programme si le code partie-programme indique une structure de type "compartimentalisation" (voir chapitre 2) : l'utilisateur n'a accès qu'au sous-programme dont le numéro est identique au CPP;

d) à plusieurs sous-programmes si le code partie-programme indique une structure de type "stratification" (voir chapitre 2) : l'utilisateur a accès au sous-programme dont le numéro est identique au CPP ainsi qu'à tous ceux dont le numéro est supérieur.

Exemples : Considérons les programmes d'application P_I et P_2 suivants :



Prenons différentes valeurs de CPP et examinons, après affectation des numéros d'ordre, quels sont les sous-programmes accessibles à l'utilisateur si nous associons au code partie-programme un flag indiquant le type de structure (compartimentalisation ou stratification) dont il faut tenir compte pour établir les autorisations de ce groupe :

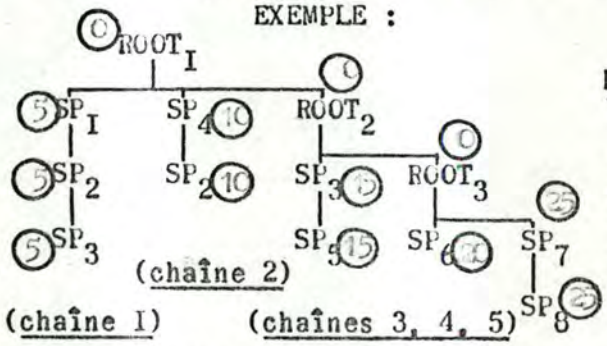


Ces exemples montrent que l'affectation de numéros d'ordre peut être réalisée de plusieurs manières.
De plus, si elle pose peu de problèmes dans le cas des structures linéaires, elle peut être diffcile à réaliser dans le cas d'une structure arborescente.
En fait, l'affectation est conditionnée par la manière dont a été réalisée là subdivision du programme en sous-programmes.

On essayera, afin de faciliter l'affectation des numéros d'ordre, de transformer la structure arborescente en un ensemble de structures linéaires.

Pratiquement, ceci revient à subdiviser le programme en un ensemble de chaînes de traitements où chacune sera une structure linéaire. Les numéros d'ordre seront affectés en considérant chaque chaîne comme un compartiment (compartimentalisation). De plus, l'entrée dans une chaîne sera toujours précédée par un sous-programme appelé $ROOT_i$, accessible sans restriction, affecté du numéro d'ordre 0.

EXEMPLE :



Note:

Le numéro d'ordre est affecté à la chaîne et est connu du moniteur précédant la chaîne; un même sous-pr. peut faire partie de plus. chaînes.

Chacun de ces $ROOT_i$ comportera :

1) les instructions d'appel aux chaînes de sous-programmes dont il contrôle l'accès,

2) les tests de correspondance entre le CPP de l'utilisateur et le numéro d'ordre de ces chaînes.

L'ensemble des $ROOT_i$ constitue le programme moniteur permettant d'effectuer le contrôle d'accès aux sous-programmes internes à un programme d'application.

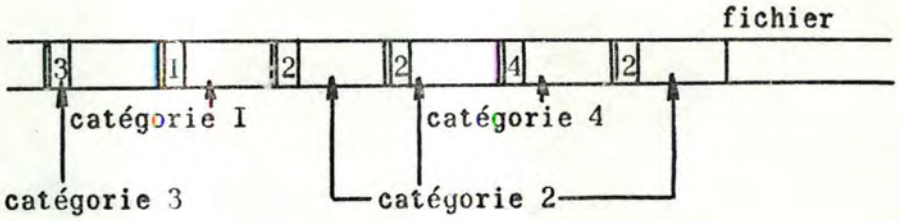
e) à plusieurs catégories d'enregistrements du fichier :

L'ensemble des enregistrements du fichier sera subdivisé en un certain nombre de catégories ; chaque catégorie est affectée d'un numéro d'ordre appelé code enregistrement (CE).

g) à une seule catégorie d'enregistrements :

Exemples:

1) en utilisant la technique de stratification, l'utilisateur a accès à tous les enregistrements ayant un code enregistrement supérieur ou égal à celui de la table. Si, par exemple, l'utilisateur a un CE_{table} de 2, il aura accès aux enregistrements des catégories 2, 3 et 4.



2) en utilisant la technique de compartimentalisation, l'utilisateur n'a accès qu'aux enregistrements dont le $CE_{enreg.}$ est identique au CE_{table} .

Dans l'exemple précédent, l'utilisateur n'aura accès qu'aux enregistrements de la deuxième catégorie.

Extensions : Si chaque item CE/CM de la table est associé, non plus à un fichier mais à une base de données, une catégorie d'enregistrements peut constituer l'ensemble des enregistrements d'un fichier. (ou d'une base de données)

Table des groupes	BASE I	BASE 2	...	...
	CE/CM	CE/CM	...	...

I.2.3. TABLE 3 : TABLE DES MASQUES.

Elle comprend autant d'entrées que de fichiers. Une entrée est constituée des items suivants :

item I : nombre de masques existant pour ce fichier.
item 2.: table des masques existants.
item 3 : nombre d'items dans l'enregistrement du fichier.
item 4 : nombre de bytes utilisés pour le masque.
item 5 : longueur de l'enregistrement du fichier.
item 6 : description de l'enregistrement (longueur des ≠ items).
item 7 à I4 : masques utilisés pour ce fichier. (2 bits par item).

fig. I.I

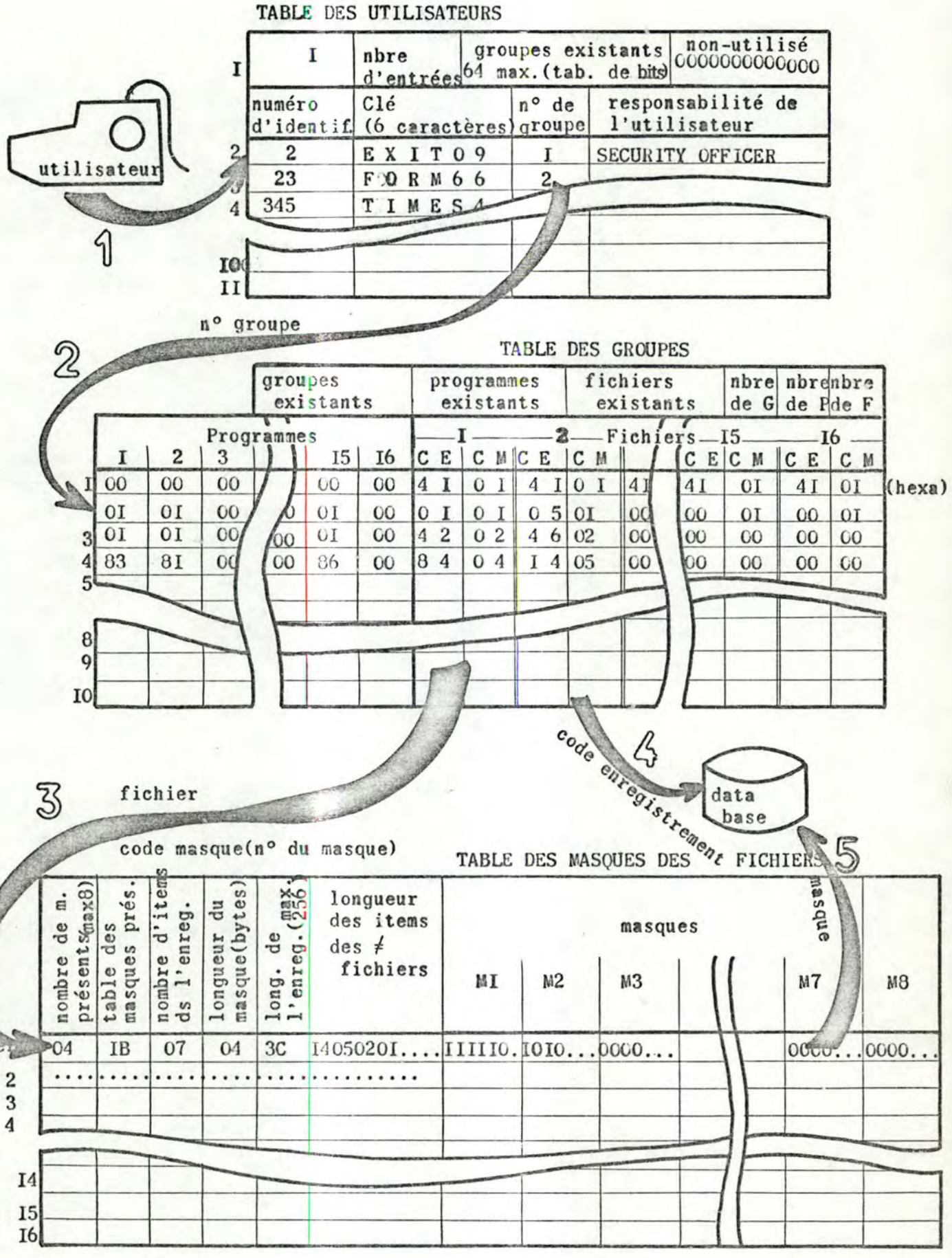


TABLE DES UTILISATEURS
I
nbre d'entrées
groupes existants 64 max. (tab. de bits)
non-utilisé 000000000000
numéro d'identif.
Clé (6 caractères)
n° de groupe
responsabilité de l'utilisateur
2
EXIT09
SECURITY OFFICER
23
FORM66
2
345
TIMES4
utilisateur
1
n° groupe
2
TABLE DES GROUPES
groupes existants
programmes existants
fichiers existants
nbre de G
nbre de P
nbre de F
Programmes
Fichiers
(hexa)
code enregistrement
4
data base
3
fichier
code masque(n° du masque)
TABLE DES MASQUES DES FICHIERS
5
nombre de m. présents (max8)
table des masques prés.
nombre d'items ds l'enreg.
longueur du masque(bytes)
long. de l'enreg.(256)
longueur des items des ≠ fichiers
masques
M1
M2
M3
M7
M8
04
1B
07
04
3C
1405020I....
IIIII0.
I0I0...
0000...
0000...
0000...

I.3. CONCLUSIONS.

1) Ce programme a été développé sans être axé vers un SGBD particulier. Il offre la possibilité de définir des autorisations d'accès à n'importe quel niveau situé depuis la base de données jusqu'aux items d'un enregistrement d'un fichier de celle-ci.

2) Pratiquement, dans une entreprise, la notion de groupe(telle que nous l'avons définie pour la table des groupes) existe toujours : nous pouvons l'assimiler à une catégorie de personnel.
Si nous supposons, par exemple, qu'il existe au maximum 8 catégories de personnel, la table des groupes comportera 8 entrées. Dès lors, 8 masques au plus, par fichier, seront suffisants pour définir les autorisations d'accès au niveau des items de chacun des enregistrements.

3) De plus, à l'aide des commandes du langage de maintenance, le responsable de la sécurité a la possibilité de mettre à jour rapidement et en temps réel, les tables de sécurité.
Remarque : Il faut toujours tenir compte que la mise en place d'un système de sécurité implique un coût supplémentaire de traitement ainsi que l'impossibilité de travailler en temps réel avec un temps de réponse très faible.

section 2 : phase de conception d'un langage de maintenance des tables de sécurité : projet "lama".

2.1. INTRODUCTION.

Lorsque d'une part, de nombreux utilisateurs ont accès aux mêmes terminaux, aux mêmes informations (programmes et données) ou aux mêmes volumes et que d'autre part, les données peuvent être subdivisées en différents niveaux de confidentialité, les tables de sécurité peuvent devenir très complexes.

De plus, si le système de sécurité doit évoluer constamment, le (¥) responsable de la sécurité doit pouvoir effectuer, rapidement et sans risque d'erreurs, toute modification à apporter aux tables de sécurité.

Exemples de modifications :

- introduction de nouveaux fichiers, de nouvelles catégories d'utilisateurs,
- changement périodique des catégories d'autorisation ou des mots de passe,
- modification des privilèges accordés aux utilisateurs.

Dans le contexte d'un système fonctionnant en télétraitement, ces modifications devront pouvoir être exécutées instantanément.

Exemple : modification de l'ensemble des mots de passe en cas de tentatives de violation de la procédure de contrôle d'accès.

L'ensemble de ces exigences justifient la conception d'un langage de maintenance destiné au responsable de la sécurité.

2.2. DESCRIPTION.

Le langage comprend deux groupes de commandes :

- les commandes de mise à jour des tables de sécurité :
  - . INSERT
  - . DELETE
  - . MODIFY
- la commande de visualisation ou d'impression des tables de sécurité
  - . COPY

Les routines permettant de traiter ces commandes devront être protégées au même titre que les routines de sécurité décrites précédemment.

(¥) La nécessité du caractère évolutif vient de ce que le système doit s'adapter à une organisation elle même en évolution et dont les composants évoluent de façon très diverse.

2.2.I. REMARQUES GENERALES.

A. COMMANDES INSERT, MODIFY, DELETE.

Chaque commande comporte un ensemble de paramètres qui peuvent être subdivisés en trois groupes.

Paramètres du groupe I :

a - présentation : /paramètre/

b - fonction : identifier la table à modifier.

Conventions : U : table des Utilisateurs.

P) : Programmes
F : Fichiers
} Table des Groupes

G : Table des groupes.

M : Table des masques.

(Remarque : L'ensemble des commandes concernant les différentes tables sont reprises face aux symboles A B ou C ou

A : désigne les commandes destinées à la table des utilisateurs.

B : désigne les commandes destinées à la table des groupes.

C.: désigne les commandes destinées à la table des masques).

Paramètres du groupe 2 :

a - présentation : /paramètre/

b - fonction : permettent de différencier les commandes agissant au niveau de la table des commandes portant sur une entrée de celle-ci.

Conventions : N : New
O : Old
) concernent un programme ou un fichier.

P : Programme (code partie programme)

E : Code enregistrement.

M. Code masque. (N° de masque)

Paramètres du groupe 3 :

a - présentation : soit {-paramètres avec virgules comme séparateurs ;
-paramètres sans virgules de part et d'autre.

b - fonction : permettent de préciser le (les) item. (s) de la table qui fait l'objet de la commande. Dans certaines commandes, ils indiquent aussi la valeur de ces items.

B. COMMANDE COPY

La commande ne contient que des paramètres du groupe I (voir ci-dessus). Elle permet d'obtenir le contenu binaire de la table indiquée par un paramètre du groupe I (voir implémentatio

2.2.2 LA COMMANDE INSERT.

a) FORME GENERALE.

(A) (I) INSERT / U / numéro d'identification / mot de passe / numéro de groupe / responsabilité de l'utilisateur

(B) (5) / P / New / numéro de programme

(B) (7) / F / New / numéro de fichier

(B) (9) / P / Program / numéro de groupe, numéro de progr., code partie-prog.

(B) (I2) / F / Enreg. / Mask / numéro de groupe, numéro de fichier, code enreg. / code masque

(C) (I5) / M / numéro de fichier, n° de masque , masque

b) SPECIFICATIONS.

-forme (I): permet d'insérer un nouvel utilisateur dans la table des utilisateurs.
(voir exemple I)

-formes (5) et (7): permettent de tenir compte de l'existence d'un nouveau programme d'application ou d'un nouveau fichier de la base de données.(exemple 5 et 7)

-forme (9): permet de donner, à un groupe, l'autorisation d'accéder à un programme d'application. La valeur du code partie-programme indique les sous-programmes accessibles à ce groupe.(exemple 9)

-forme (I2): permet de donner, à un groupe, l'autorisation d'accéder à l'un des fichiers de la base de données.
La valeur du code enregistrement indique les enregistrement de ce fichier qui sont accessibles à ce groupe.
La valeur du code masque indique , pour chacun de ces enregistrements, les items accessibles à ce groupe en lecture, en écriture ou en modification.(exemple I2)

(Note: les formes (5),(7),(9) et (I2) se rapportent à la table des groupes).

-forme (I5): par cette commande, le responsable de la sécurité a la possibilité d'ajouter un nouveau masque dans la liste des masques d'un fichier.(exemple I5)

c) EXEMPLES:

(I) INSERT/U/0002,EXITO90,SECURITY OFFICER
(5) INSERT/P/N/08
(7) INSERT/F/N/02
(9) INSERT/P/P/02,01,20
(I2) INSERT/F/E/02,05,005
INSERT/F/M/02,05,02
(I5) INSERT/M/12,03,CCIIOIIOIOIOOOOOOOOOIOIIOOIIOOOOOOOO

(voir aussi ch. IV,section 2: phase d'implémentation du langage "LAMA")

2.2.3 LA COMMANDE DELETE.

a) FORME GENERALE.

(A)	(2)	D E L E T E	/ U / numéro d'identification
	(6)		/ P / Old / numéro de programme
	(8)		/ F / Old / numéro de fichier
(B)	(I0)		/ P / Programme / numéro de groupe , numéro de programme
	(I3)		/ F / Enreg. / numéro de groupe , code enregistrement / Mask / n°groupe , code masque
(C)	(I6)		/ M / n° de fichier, n° de masque
(B)	(I8)		/ G / n° de groupe

b) SPECIFICATIONS.

-forme (2): permet de supprimer un utilisateur dans la table des utilisateurs.(exemple 2)

-formes (6) et (8): permettent de supprimer un programme d'application ou un fichier. Ces commandes entraînent automatiquement la suppression de tous les codes (partie-programme, enreg. et masque) dans la colonne de la table correspondant à ce programme ou à ce fichier.(exemple 6 et 8)

-formes (I0) et (I3): permettent de supprimer soit un code partie-prog., soit un code enregistrement ou masque, à l'intérieur d'une seule entrée (groupe) de la table des groupes. En fait, elles retirent ,à un groupe son autorisation d'accéder à un programme d'application ou à un fichier.(exemples I0 et I3)

-forme (I8): par cette commande, le responsable de la sécurité a la possibilité de supprimer l'entrée correspondant à un groupe d'utilisateurs. Elle supprime donc un groupe et tous les privilèges qui lui étaient associés.

-forme (I6): cette commande est destinée à supprimer l'un des masques associés à un fichier de la base de données. La suppression ne sera effectuée que si la table des groupes n'y fait plus référence.(exemple I6)

c) EXEMPLES:

(2)	DELETE/U/0I2I
(6)	DELETE/P/Ø/02
(8)	DELETE/F/Ø/03
(I0)	DELETE/P/P/02,04
(I3)	DELETE/F/E/02,05
(I6)	DELETE/F/M/02,05
	DELETE/M/I2,01
(I8)	DELETE/G/04

(Voir aussi ch. IV, section 2: phase d'implémentation)

2.2.4 LA COMMANDE MODIFY.

a) FORME GENERALE.

(A) (3) M O D I F Y / U / numéro d'identification, de la table { N , nouveau num. d'ident. | K , nouvelle clé | G , nouveau groupe | R , nouvelle responsabil. }

(B) (II) / P / Progr. / numéro de groupe , numéro de programme , code partie programme

(B) (I4) / F { / Enreg. / | / Mask / } numéro de groupe , numéro de fichier , { code enreg. | code masque }

(C) (I7) / M / numéro de fichier , numéro de masque , masque

b) SPECIFICATIONS.

-forme (3): par cette commande, le responsable de la sécurité a la possibilité de modifier l'un des items d'une entrée de la table des utilisateurs.(exemple 3)
La modification ou l'insertion d'un numéro d'identification ou d'un mot de passe sera effectuée s'il n'existe aucun numéro ou mot de passe identique dans la table.

-forme (II),et (I4): permettent de modifier les autorisations d'un groupe. La modification du code masque sera effectuée s'il existe un masque correspondant au fichier.
(exemple II et I4)

-forme (I7): cette commande est destinée à modifier l'un des masques de la table des masques. Elle modifie donc les autorisation de tous les groupes subordonnés à l'utilisation de ce masque.(exemple I7)

c) EXEMPLES:

(3)
```
MODIFY/U/0519,N,0502
MODIFY/U/0502,K,FLAG40
MODIFY/U/0502,G,02
MODIFY/U/0502,R,PROGRAMMER
```

(II)
```
MODIFY/P/P/02,04,20
```

(I4)
```
MODIFY/F/E/02,05,005
MODIFY/F/M/02,05,02
```

(voir aussi ch. IV,section 2:phase d'implémentation)

(I7)
```
MODIFY/M/02,04,0000IOIOIOIOIIIOOIIOOOIOIOIIOIIOII
```

2.2.5 REMARQUE.

Le numéro d'identification, le numéro de groupe, de programme, de fichier et de masque seront fournis en décimal.
Les codes partie-programme, enregistrement et masque seront introduits en décimal tout en tenant compte de leur présentation binaire dans la table (positionnement des bits 8 et 7 -voir commentaires associés à la table des groupes). Le masque sera introduit sous forme d'une chaîne de caractères I et O.

CHAPITRE 4 :
implémentation d'un programme de contrôle d'accès (niveau de la gestion des opérations)

section 1 : phase d'implémentation des fonctions d'identification, d'autorisation et de contrôle.

I.I. REMARQUES GENERALES.

Les routines de sécurité peuvent soit :

- faire partie intégralement du système ,
- être séparées du système d'exploitation, sous forme d'une série de processus.

Cette dernière solution , retenue par la plupart des constructeurs, présente l'avantage de pouvoir élaborer le système de sécurité en fonctions des exigences de l'installation.

Quelle que soit la solution retenue, elles doivent être conçues de façon à pouvoir, à tout moment, valider tout accès au système.

Dans les systèmes d'ordinateur fonctionnant en télétraitement, elles seront-résidentes en mémoire centrale.

- implémentées à deux niveaux différents :

  . au niveau de la gestion des messages,
  . au niveau de la gestion des données.

La Fig. I.I. permet d'illustrer cette implémentation :

a) Au niveau de la gestion des messages, tout message sera contrôlé avant qu'il ne puisse accéder aux programmes d'application.

   Les routines de sécurité détermineront :

   -d'une part, l'identification de l'utilisateur et/ou du terminal qui est à l'origine du message,

   -d'autre part, si l'utilisateur ou le terminal a l'autorisation d'accéder au programme d'application qu'il demande.

   Toute tentative de violation des routines de sécurité (procédures d'identification et d'autorisation) sera enregistrée (LOGGING) afin d'être ultérieurement analysée par le responsable de la sécurité.

b) Au niveau de la gestion des données, toute demande de consultation ou de modification de la base de données sera contrôlée préalablement à tout accès aux enregistrements faisant l'objet de cette demande.

   Lors d'une demande de consultation, si l'autorisation d'accéder à un enregistrement dépend du contenu de celui-ci (c'est-à-dire, de la valeur d'un item) ou du nombre d'enregistrements faisant l'objet de la demande (ex. : établissement de relevés statistiques),

les routines de sécurité devront préalablement contrôler le contenu de celui-ci en fonction de critères prédéterminés, (présentés, par exemple, sous forme d'une table de décision). Si ces critères sont respectés, l'enregistrement sera disponible au programme d'application.

Note : Si l'utilisateur n'a accès qu'à certains items de l'enregistrement, les routines de sécurité devront :

- masquer ceux-ci (lors d'une consultation) avant de rendre l'enregistrement disponible au programme ;
- éviter tout accès à ceux-ci lors d'une modification .

Résumé : Tout message entrant dans le système sera analysé par les routines de sécurité implémentées au niveau de la gestion des messages.

Tout programme ne pourra accéder à la base de données qu'en passant par les routines de sécurité implémentées au niveau de la gestion des données.

REMARQUES : Au niveau de la mémoire centrale, les programmes d'application seront :

a. séparés des programmes superviseur :

. Il faudra s'assurer qu'aucun programme d'application ne puisse : . soit passer de l'état "problème" à l'état"superviseur",

. soit exécuter des instructions privilégiées,

. soit lire des informations (mots de passe, codes de sécurité) dans la zone mémoire réservée au superviseur.

b. isolés les une des autres au moyen :

. de la protection mémoire (storage protection) : consiste en une protection d'écriture ;

. de la fetch-protection : consiste en une protection de lecture.

I.2. STRUCTURE GENERALE DU PROGRAMME DE CONTROLE D'ACCES.(fig. I.2)

Le programme de contrôle d'accès est subdivisé en quatre routines de sécurité.

I) CSMAIN (niveau gestion des messages)

. assure les fonctions :

- d'identification : traitement des commandes d'identification (cartes ADRESS, LOGON, KEY) par un test de correspondance entre "NI/KEY" fourni par l'utilisateur et "NI/KEY" de la table des utilisateurs.

- d'autorisation : traitement des messages (cartes PROG, READ, WRITE, UPDATE, LIST).
- de contrôle : impression d'un message sur le terminal du responsable de la sécurité en cas de tentatives de violation.

2) CSECT I, 2, 3 (niveau gestion des données)

. voir section 2.

3) CSECT 4

. vidage d'un fichier indexé séquentiel.

4) CSECT 5

. création d'un fichier indexé séquentiel.

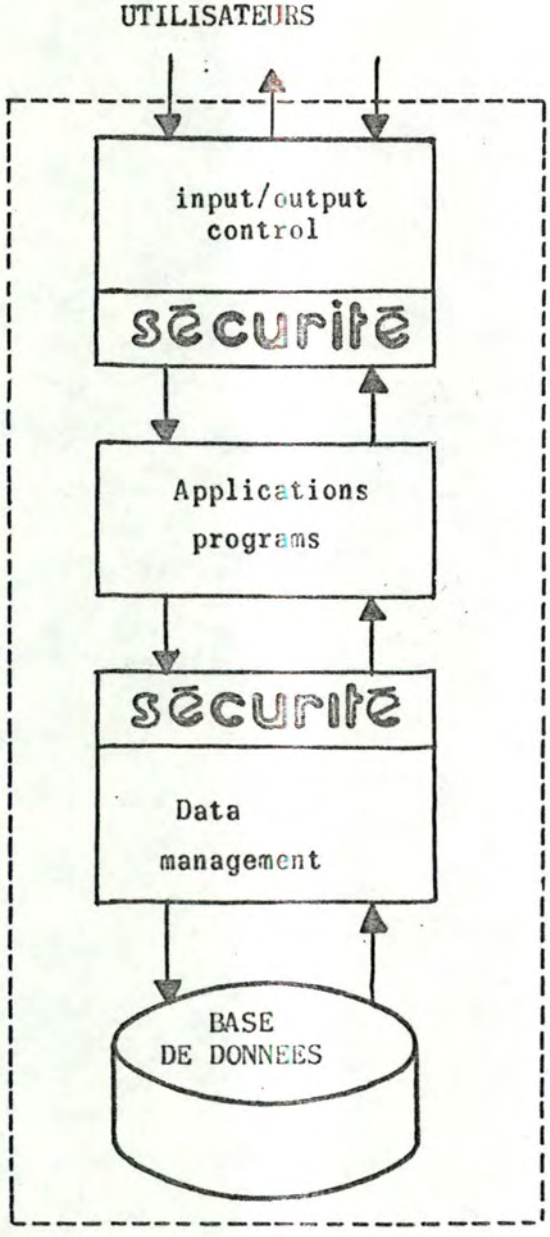


fig. I.I

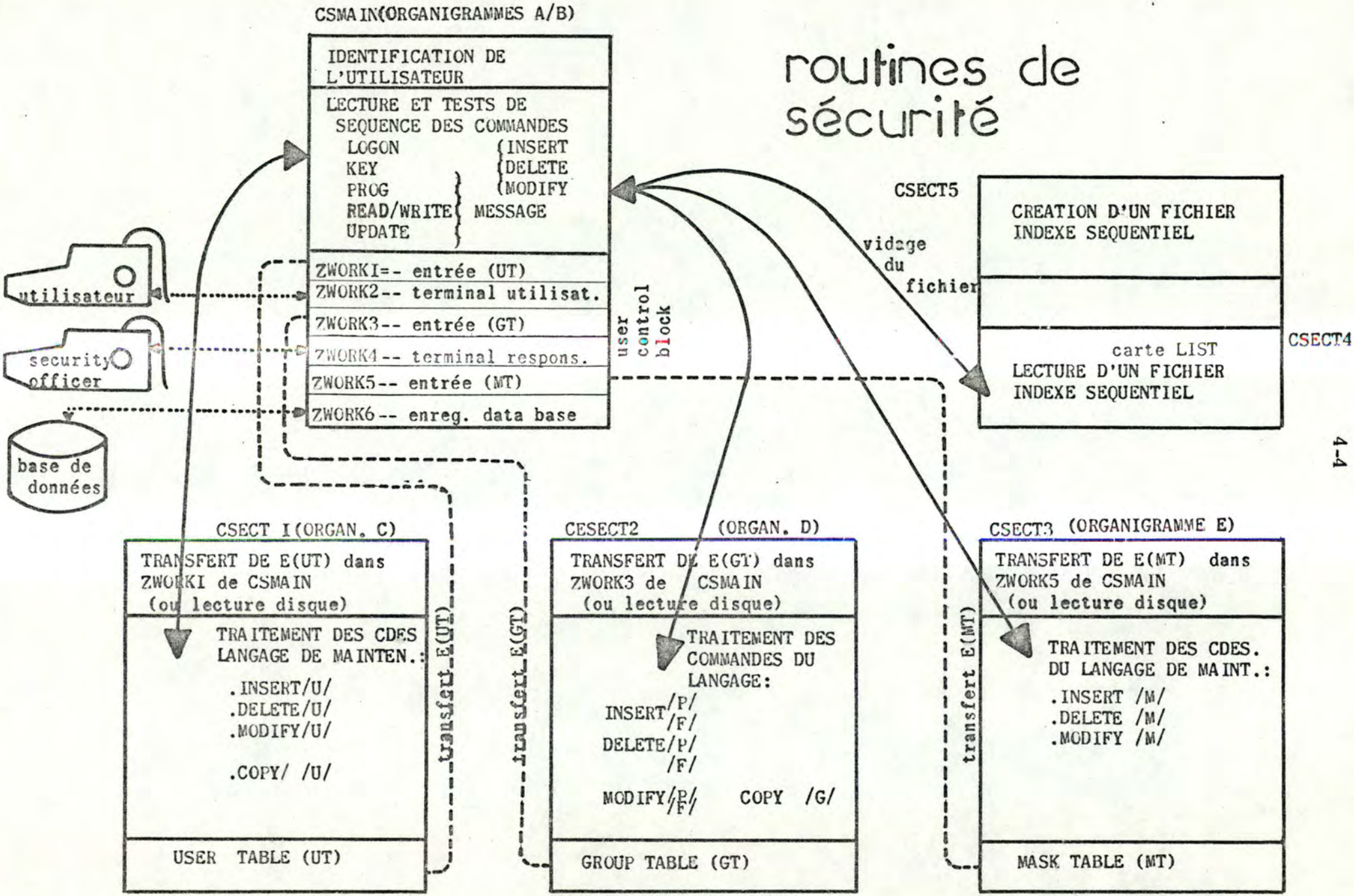
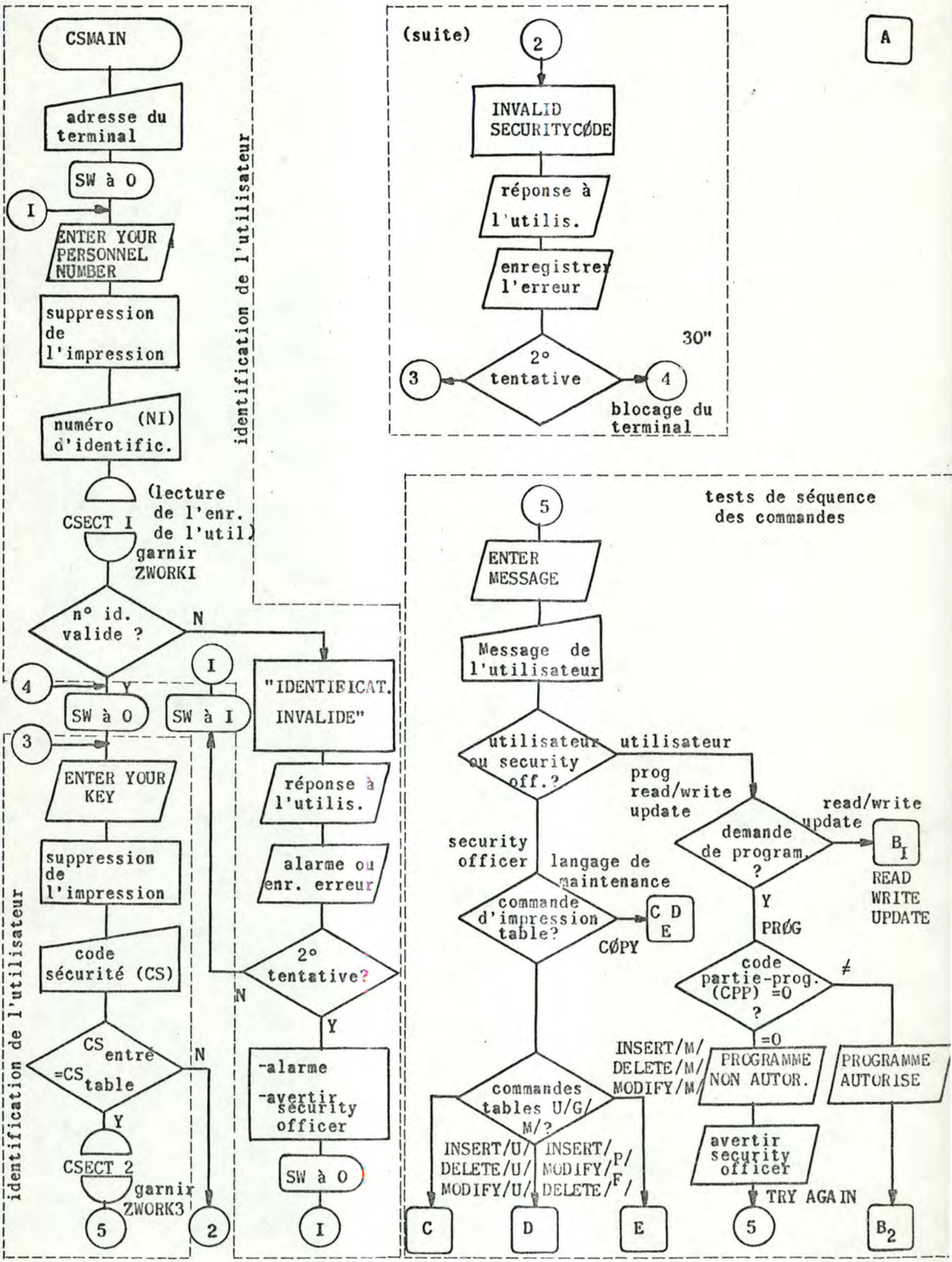
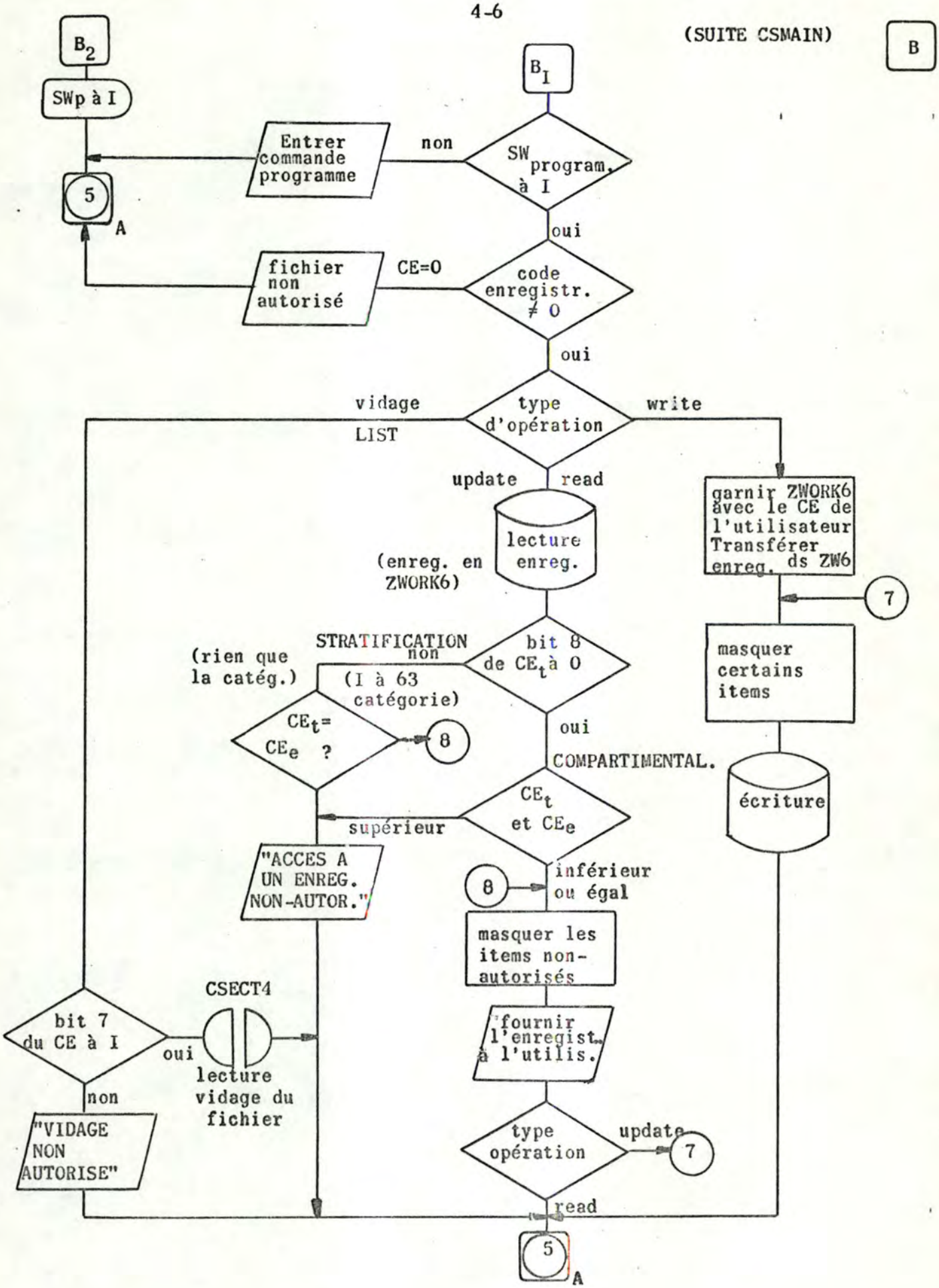

CSMAIN(ORGANIGRAMMES A/B)
IDENTIFICATION DE L'UTILISATEUR
LECTURE ET TESTS DE SEQUENCE DES COMMANDES
LOGON
KEY
PROG
READ/WRITE
UPDATE
INSERT
DELETE
MODIFY
MESSAGE
ZWORK1=- entrée (UT)
ZWORK2-- terminal utilisat.
ZWORK3-- entrée (GT)
ZWORK4-- terminal respons.
ZWORK5-- entrée (MT)
ZWORK6-- enreg. data base
user control block
routines de sécurité
CSECT5
CREATION D'UN FICHIER INDEXE SEQUENTIEL
vidage du fichier
carte LIST
LECTURE D'UN FICHIER INDEXE SEQUENTIEL
CSECT4
utilisateur
security officer
base de données
CSECT I(ORGAN. C)
TRANSFERT DE E(UT) dans ZWORK1 de CSMAIN (ou lecture disque)
TRAITEMENT DES CDES LANGAGE DE MAINTEN.:
.INSERT/U/
.DELETE/U/
.MODIFY/U/
.COPY/ /U/
USER TABLE (UT)
transfert E(UT)
CESECT2 (ORGAN. D)
TRANSFERT DE E(GT) dans ZWORK3 de CSMAIN (ou lecture disque)
TRAITEMENT DES COMMANDES DU LANGAGE:
INSERT/P/ /F/
DELETE/P/ /F/
MODIFY/P/ /F/
COPY /G/
GROUP TABLE (GT)
transfert E(GT)
CSECT3 (ORGANIGRAMME E)
TRANSFERT DE E(MT) dans ZWORK5 de CSMAIN (ou lecture disque)
TRAITEMENT DES CDES. DU LANGAGE DE MAINT.:
.INSERT /M/
.DELETE /M/
.MODIFY /M/
MASK TABLE (MT)
transfert E(MT)

fig. I.2


CSMAIN
adresse du terminal
SW à 0
I
ENTER YOUR PERSONNEL NUMBER
suppression de l'impression
numéro (NI) d'identific.
CSECT I
(lecture de l'enr. de l'util.)
garnir ZWORKI
identification de l'utilisateur
n° id. valide ?
N
Y
4
SW à 0
SW à I
I
"IDENTIFICAT. INVALIDE"
réponse à l'utilis.
alarme ou enr. erreur
2° tentative?
N
Y
-alarme
-avertir security officer
SW à 0
I
3
ENTER YOUR KEY
suppression de l'impression
code sécurité (CS)
CS entré =CS table
N
Y
CSECT 2
garnir ZWORK3
5
2
identification de l'utilisateur
(suite)
2
INVALID SECURITYCODE
réponse à l'utilis.
enregistrer l'erreur
30"
2° tentative
3
4
blocage du terminal
A
tests de séquence des commandes
5
ENTER MESSAGE
Message de l'utilisateur
utilisateur ou security off.?
utilisateur
prog read/write update
security officer
langage de maintenance
demande de program. ?
read/write update
B I
READ WRITE UPDATE
commande d'impression table?
C D E
COPY
Y
PRØG
code partie-prog. (CPP) =0 ?
≠
=0
commandes tables U/G/M/?
INSERT/M/ DELETE/M/ MODIFY/M/
PROGRAMME NON AUTOR.
PROGRAMME AUTORISE
INSERT/U/ DELETE/U/ MODIFY/U/
INSERT/P/ MODIFY/F/ DELETE/F/
avertir security officer
TRY AGAIN
C
D
E
5
B2

(SUITE CSMAIN)



OUTPUT CSMAIN (voir organigramme A et B)

Identification de l'utilisateur.

Autorisation.

CONSOLE DE L'UTILISATEUR

CONSOLE DU RESPONSABLE DE LA SECURITE

```
ADRESS A005
                                        TA A005   **TERMINAL ADRESS  A005***TEST********

>ENTER YOUR PERSONNEL NUMBER
LOGON  1024

>ENTER YOUR KEY
KEY    FIELD1
***INVALID SECURITY CODE
                                        TA A005   ***INVALID  PASSWORD/KEY(FIELD1)
>ENTER YOUR KEY            (TRY AGAIN!)
KEY    PERSON

>ENTER MESSAGE
PROG   09
***UNAUTHORIZED PROG.
                                        TA A005   TENTATIVE D'ACCES A UN PROG(09)  INT.
                                        TA A005       PROG   09
                                        TA A005       NI/1024 KEY/PERSON
                                        TA A005       RESPONSABILITY/ DP MANAGEMENT

>ENTER MESSAGE
PROG   02
PROG. 02 AUTHORIZED(CPP 001)
```

(Groupe 3)
Masque fichier OI: (code masque 02)

	IO	IO	II	II	II	II	II	00	00
items	I	2	3	4	5	6	7	8	9 .....

Code enregistrement: 42 (base I6)

```
>ENTER MESSAGE
WRITE  01 2030|LLLLLLLLLLLLLLLLLLL|11111|22|3|4|55555555555555555555|6666|

>ENTER MESSAGE
READ   01 2030
2030|**********************|*****|22|3|4|55555555555555555555|6666| **********
          item I                item 2
```

(autorisation d'écrire les items 3,4,5,6 et 7)

```
>ENTER MESSAGE
READ   01 2500
***UNAUTHORIZED RECORD
                                        TA A005   TENTATIVE D'ACCES A UN ENREG. INT.
                                        TA A005       READ   01 2500
                                        TA A005       NI/1024 KEY/PERSON
                                        TA A005       RESPONSABILITY/ DP MANAGEMENT
```

(le bit 8 du CE est à 0, ce qui signifie: "COMPARTIMENTALISATION". Cet utilisateur n'a accès qu'aux enregistrements dont le CE est 2)

(code enregistrement: 4 2 ([0100] [0010])$_2$

```
>ENTER MESSAGE
COPY   /G/
NO UPDATE PROCEDURE AVAILABLE
```

(commande réservée au responsable de la sécurité)

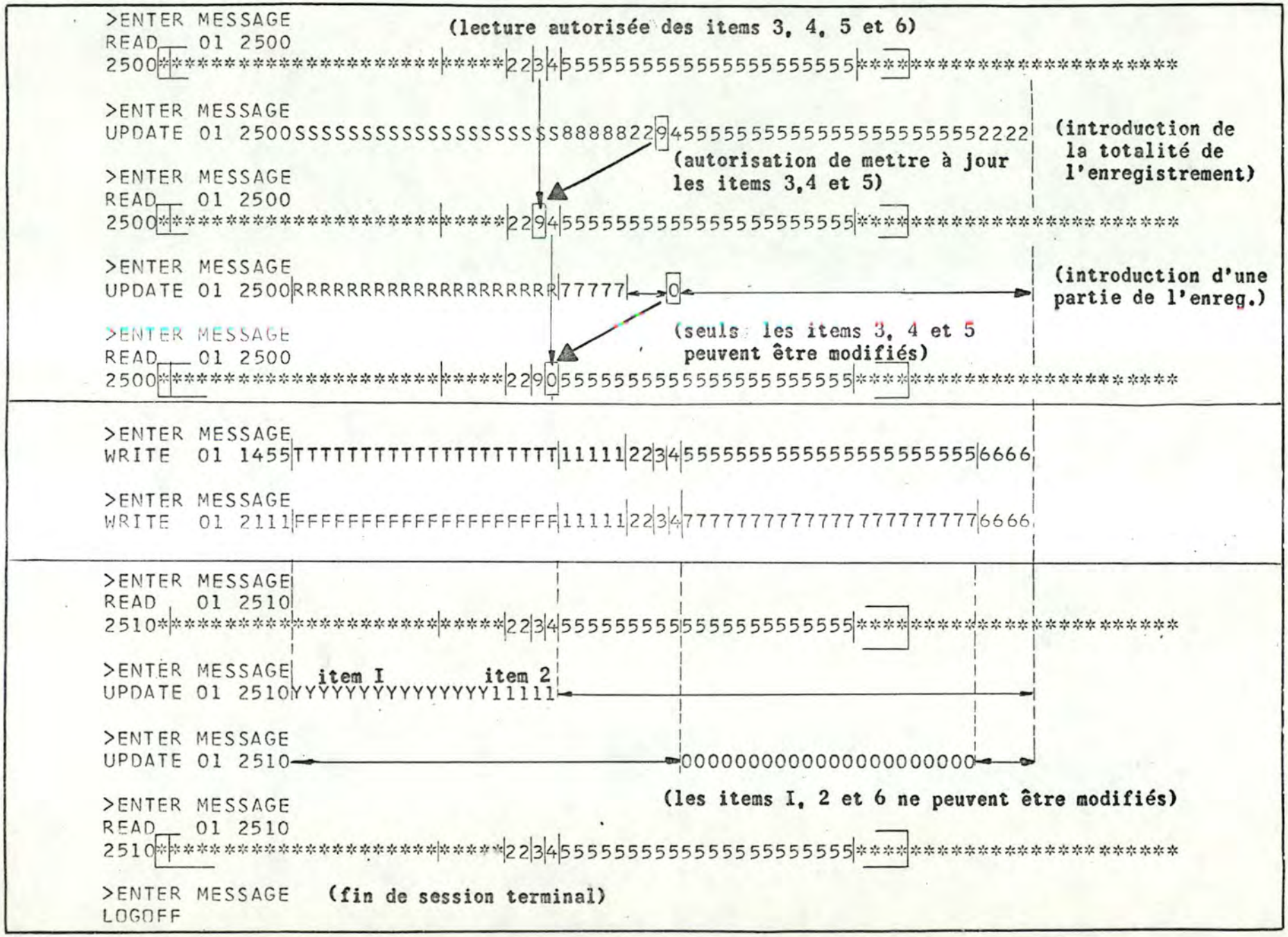
(output CSMAIN -suite)

```
>ENTER MESSAGE
LIST   01

                                                    TA A005   ****VIDAGE DU FICHIER 01***
|1000|1|AAAAAAAAAAAAAAAAAAAA|11111|22|34|55555555555555555555|6666|
|1012|5|BBBBBBBBBBBBBBBBBBBB|11111|22|34|55555555555555555555|6666|
|1015|4|CCCCCCCCCCCCCCCCCCCC|11111|22|34|55555555555555555555|6666|
|1050|2|DDDDDDDDDDDDDDDDDDDD|11111|22|34|55555555555555555555|6666|
|1110|1|EEEEEEEEEEEEEEEEEEEE|11111|22|34|55555555555555555555|6666|
|1125|2|FFFFFFFFFFFFFFFFFFFF|11111|22|34|55555555555555555555|6666|
|1400|1|GGGGGGGGGGGGGGGGGGGG|11111|22|34|55555555555555555555|6666|
|1430|5|HHHHHHHHHHHHHHHHHHHH|11111|22|34|55555555555555555555|6666|
|1435|5|IIIIIIIIIIIIIIIIIIII|11111|22|34|55555555555555555555|6666|
|1450|3|JJJJJJJJJJJJJJJJJJJJ|11111|22|34|55555555555555555555|6666|
|2000|4|KKKKKKKKKKKKKKKKKKKK|11111|22|34|55555555555555555555|6666|
|2030|2|********************|22|34|55555555555555555555|6666|
|2305|2|MMMMMMMMMMMMMMMMMMMM|11111|22|34|55555555555555555555|6666|
|2500|4|MMMMMMMMMMMMMMMMMMMM|11111|22|34|55555555555555555555|6666|
|2505|5|NNNNNNNNNNNNNNNNNNNN|11111|22|34|55555555555555555555|6666|
|2508|5|OOOOOOOOOOOOOOOOOOOO|11111|22|34|55555555555555555555|6666|
|2509|5|QQQQQQQQQQQQQQQQQQQQ|11111|22|34|55555555555555555555|6666|
|2510|4|XXXXXXXXXXXXXXXXXXXX|11111|22|34|55555555555555555555|6666|
|2680|3|ZZZZZZZZZZZZZZZZZZZZ|11111|22|34|55555555555555555555|6666|
|4550|5|TTTTTTTTTTTTTTTTTTTT|11111|22|34|55555555555555555555|6666|
|4800|5|ZZZZZZZZZZZZZZZZZZZZ|11111|22|34|55555555555555555555|6666|
                                                    TA A005        NI/1024 KEY/PERSON
                                                    TA A005        RESPONSABILITY/ DP MANAGEMENT

>ENTER MESSAGE
LOGOFF                    (fin de la session terminal de cet utilisateur)

ADRESS A001
                                                    TA A001   **TERMINAL ADRESS  A001***TEST********

>ENTER YOUR PERSONNEL NUMBER
LOGON  0549
                          (début de la session terminal de cet utilisateur)
>ENTER YOUR KEY
KEY    FLAG33

>ENTER MESSAGE
PROG   01
PROG. 01 AUTHORIZED(CPP 083)
```

(vidage autorisé car bit 7 du CE positionné à I)

(le bit 8 du code enregistrement (CE) est à I, ce qui signifie: "STRATIFICATION". L'utilisateur a accès aux enreg. dont leur codes est ≥4.

(Groupe 4)
Masque fichier 01: (code masque 04)
00 00 II II II I0 0I 00 00 00 .....
items I 2 3 4 5 6 7 .....


>ENTER MESSAGE
READ 01 2500
(lecture autorisée des items 3, 4, 5 et 6)
2500*****22345555555555555555555*****
>ENTER MESSAGE
UPDATE 01 2500SSSSSSSSSSSSSSSSSS8888822945555555555555555555552222
(introduction de la totalité de l'enregistrement)
(autorisation de mettre à jour les items 3,4 et 5)
>ENTER MESSAGE
READ 01 2500
2500*****22945555555555555555555*****
>ENTER MESSAGE
UPDATE 01 2500RRRRRRRRRRRRRRRRRR77777 0
(introduction d'une partie de l'enreg.)
>ENTER MESSAGE
READ 01 2500
(seuls les items 3, 4 et 5 peuvent être modifiés)
2500*****22905555555555555555555*****
>ENTER MESSAGE
WRITE 01 1455TTTTTTTTTTTTTTTTTTT11111223455555555555555555556666
>ENTER MESSAGE
WRITE 01 2111FFFFFFFFFFFFFFFFFF11111223477777777777777777776666
>ENTER MESSAGE
READ 01 2510
2510*****2234555555555555555555*****
>ENTER MESSAGE
item I
item 2
UPDATE 01 2510YYYYYYYYYYYYYYY11111
>ENTER MESSAGE
UPDATE 01 2510000000000000000000
(les items I, 2 et 6 ne peuvent être modifiés)
>ENTER MESSAGE
READ 01 2510
2510*****22345555555555555555555*****
>ENTER MESSAGE
(fin de session terminal)
LOGOFF

```
ADRESS A005
                                                TA A005   **TERMINAL ADRESS  A005***TEST***

>ENTER YOUR PERSONNEL NUMBER
LOGON  1024

>ENTER YOUR KEY
KEY    PERSON

>ENTER MESSAGE
PROG   02
PROG. 02 AUTHORIZED(CPP 001)
```

(voir pages précédentes)

```
>ENTER MESSAGE
LIST   01
                                                TA A005   ****VIDAGE DU FICHIER 01****
|1000|1|AAAAAAAAAAAAAAAAAAAA|11111|22|34|555555555555555555555|6666|
|1012|5|BBBBBBBBBBBBBBBBBBB|11111|22|34|555555555555555555555|6666|
|1015|4|CCCCCCCCCCCCCCCCCCC|11111|22|34|555555555555555555555|6666|
|1050|2|DDDDDDDDDDDDDDDDDDD|11111|22|34|555555555555555555555|6666|
|1110|1|EEEEEEEEEEEEEEEEEEE|11111|22|34|555555555555555555555|6666|
|1125|2|FFFFFFFFFFFFFFFFFFF|11111|22|34|555555555555555555555|6666|
|1400|1|GGGGGGGGGGGGGGGGGGG|11111|22|34|555555555555555555555|6666|
|1430|5|HHHHHHHHHHHHHHHHHHH|11111|22|34|555555555555555555555|6666|
|1435|5|IIIIIIIIIIIIIIIIIII|11111|22|34|555555555555555555555|6666|
|1450|3|JJJJJJJJJJJJJJJJJJJ|11111|22|34|555555555555555555555|6666|
|1455|4|**********************|*****|22|34|**********************|6666| (voir page 3)
|2000|4|KKKKKKKKKKKKKKKKKKK|11111|22|34|555555555555555555555|6666|
|2030|2|**********************|*****|22|34|555555555555555555555|6666| (voir page I)
|2111|4|**********************|*****|22|34|**********************|6666| (voir page 3)
|2305|2|MMMMMMMMMMMMMMMMMMM|11111|22|34|555555555555555555555|6666|
|2500|4|MMMMMMMMMMMMMMMMMMM|11111|22|94|555555555555555555555|6666|
|2505|5|NNNNNNNNNNNNNNNNNNN|11111|22|34|555555555555555555555|6666|
|2508|5|OOOOOOOOOOOOOOOOOOO|11111|22|34|555555555555555555555|6666|
|2509|5|QQQQQQQQQQQQQQQQQQQ|11111|22|34|555555555555555555555|6666|
|2510|4|XXXXXXXXXXXXXXXXXXX|11111|22|34|555555555555555555555|6666|
|2680|3|ZZZZZZZZZZZZZZZZZZZ|11111|22|34|555555555555555555555|6666|
|4550|5|TTTTTTTTTTTTTTTTTTT|11111|22|34|555555555555555555555|6666|
|4800|5|ZZZZZZZZZZZZZZZZZZZ|11111|22|34|555555555555555555555|6666|
                                                TA A005        NI/1024 KEY/PERSON
                                                TA A005        RESPONSABILITY/ DP MANAGEMENT
```

(output CSMAIN -suite)

```
>ENTER MESSAGE
READ   01 1050
```

(par mesure de sécurité, le CE de l'enreg. n'e… …s fourni lors d'un read)

```
|1050|*|DDDDDDDDDDDDDDDDDDD|11111|22|34|555555555555555555555|6666| **********************
```

(output CSMAIN - suite)

```
>ENTER MESSAGE
UPDATE 01 2111FFFFFFFFFFFFFFFFFF1111122346666666666666666666666666
***UNAUTHORIZED RECORD
   (l'utilisateur ne peut mettre à jour cet
   enregistrement vu que le code enreg. (CE)
   est ≠ du sien)                          TA A005   TENTATIVE D'ACCES A UN ENREG. INT.
                                           TA A005       UPDATE 01 2111FFFFFFFFFFFFFFFF
                                           TA A005       NI/1024 KEY/PERSON
                                           TA A005       RESPONSABILITY/ DP MANAGEMENT

>ENTER MESSAGE
UPDATE 01 2030LLLLLLLLLLLLLLLLLL11111223499999999999999999996666

>ENTER MESSAGE                                  (autorisation d'écrire ou de modifier les
READ   01 2030                                   items 3,4, 5,6 et 7)
2030**********************22349999999999999999996666 ******************

>ENTER MESSAGE                                  (enreg. n'existant pas dans le fichier)
READ   01 8585
***NO RECORD FOUND OR DUPLICATE KEY/      ******,UNREACHBLE BLCK,**************,BISAM
***READ OR WRITE ABNORMALLY TERMINATED

>ENTER MESSAGE
LIST   01

                                           TA A005   ****VIDAGE DU FICHIER 01***
1000 1AAAAAAAAAAAAAAAAAAA11111 22 34 55555555555555555555 6666
1012 5BBBBBBBBBBBBBBBBBBB11111 22 34 55555555555555555555 6666
1015 4CCCCCCCCCCCCCCCCCCC11111 22 34 55555555555555555555 6666
1050 2DDDDDDDDDDDDDDDDDDD11111 22 34 55555555555555555555 6666
1110 1EEEEEEEEEEEEEEEEEEE11111 22 34 55555555555555555555 6666
1125 2FFFFFFFFFFFFFFFFFFF11111 22 34 55555555555555555555 6666
1400 1GGGGGGGGGGGGGGGGGGG11111 22 34 55555555555555555555 6666
1430 5HHHHHHHHHHHHHHHHHHH11111 22 34 55555555555555555555 6666
1435 5IIIIIIIIIIIIIIIIIIII11111 22 34 55555555555555555555 6666
1450 3JJJJJJJJJJJJJJJJJJJJ11111 22 34 55555555555555555555 6666
1455 4********************22 34 ********************6666
2000 4KKKKKKKKKKKKKKKKKK11111 22 34 55555555555555555555 6666
2030 2**********************22 34 99999999999999999999 6666
2111 4**********************22 34 ********************6666
2305 2MMMMMMMMMMMMMMMMMMM11111 22 34 55555555555555555555 6666
2500 4MMMMMMMMMMMMMMMMMMM11111 22 94 55555555555555555555 6666
2505 7NNNNNNNNNNNNNNNNNNN11111 22 34 55555555555555555555 6666
     0000000 11111 22 34 55555555555555555555
```

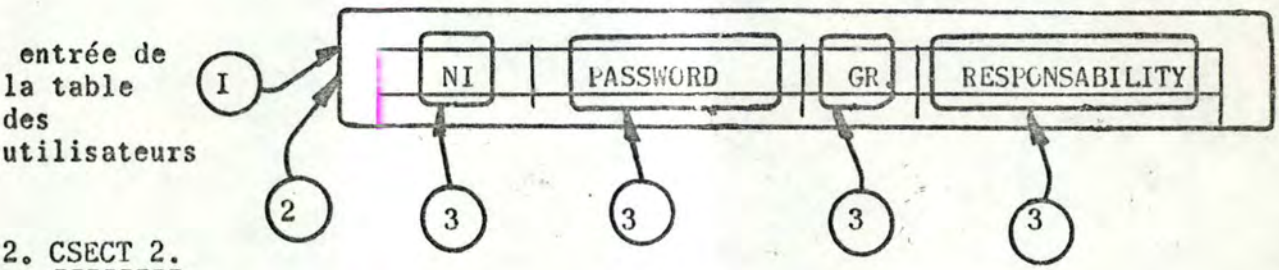
section 2 : phase d'implémentation du langage " lama ".

I.I. CSECT I.

Fonction: -Mise à jour de la table des utilisateurs.

Description: -(Voir organigramme C)

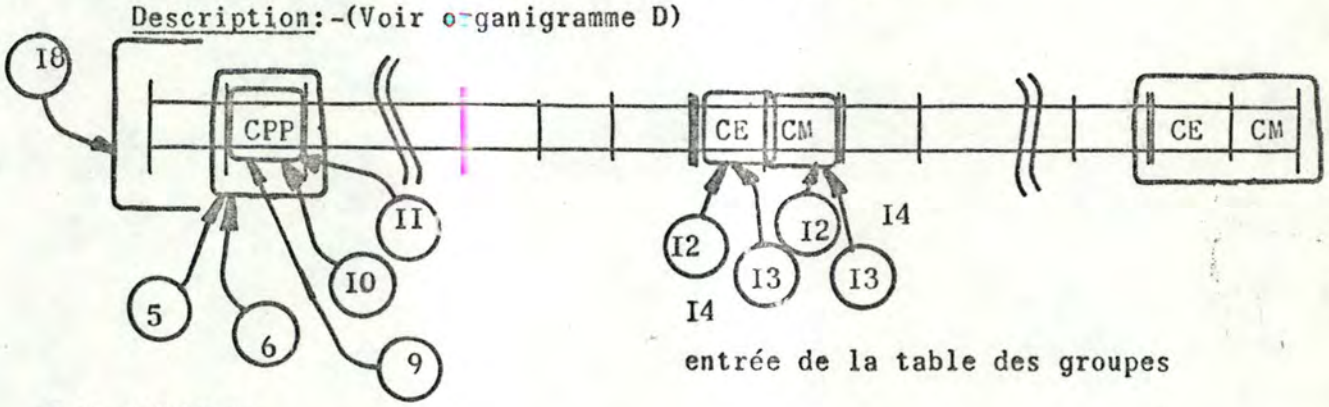
-Traitement des commandes: (voir description des commandes dans la phase de conception du langage).



I.2. CSECT 2.

Fonction: -Mise à jour de la table des groupes.

Description: -(Voir organigramme D)



I.3. CSECT 3.

Fonction: -Mise à jour de la table des masques.

Description: -(Voir organigramme E)

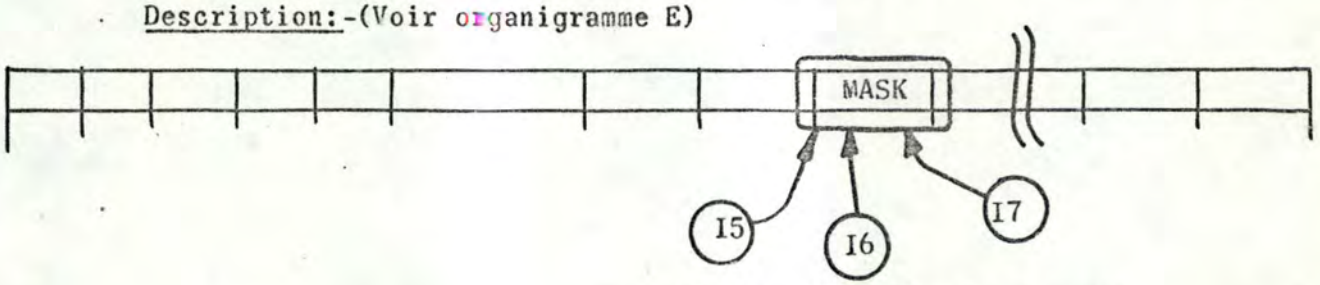
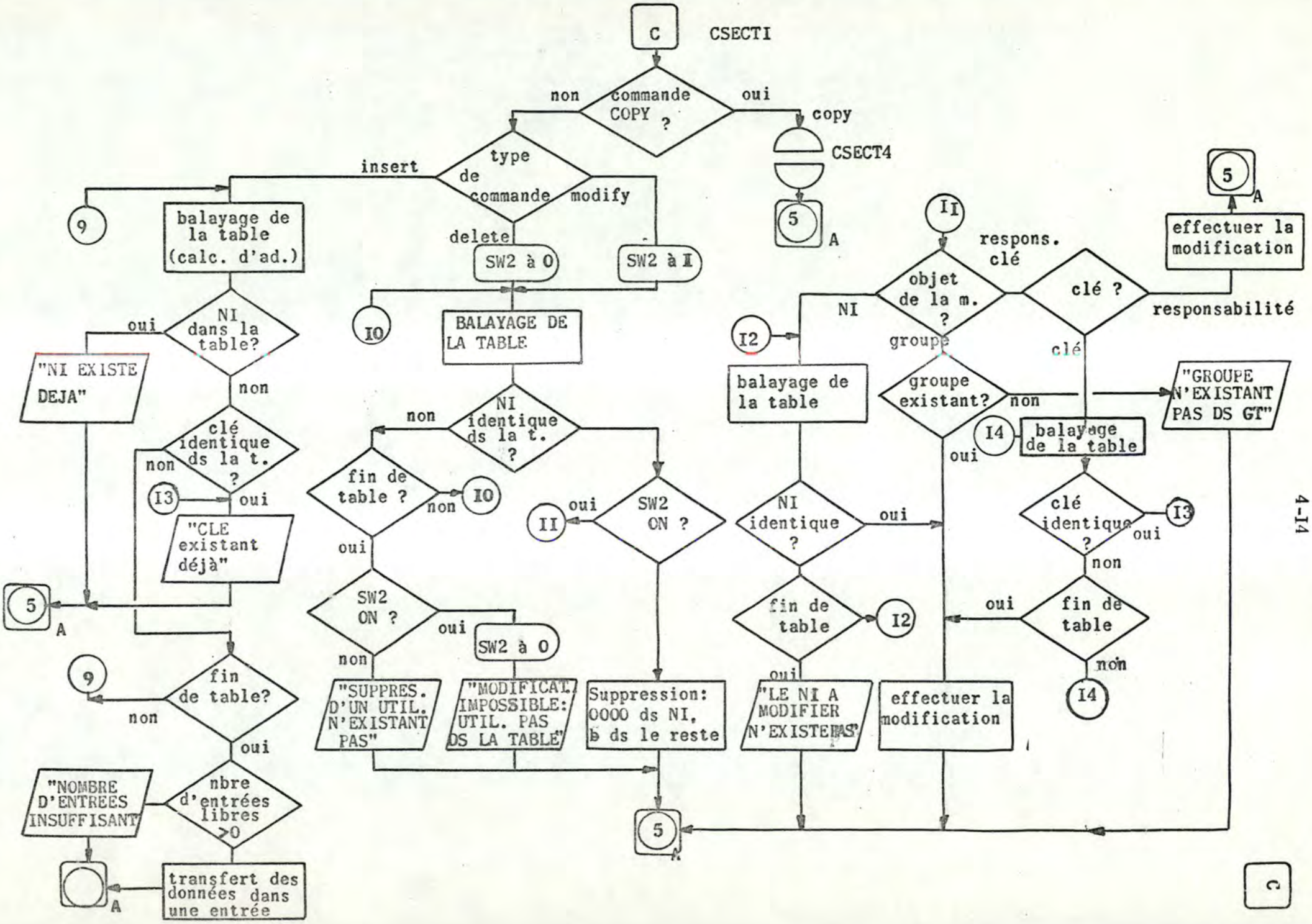


TABLE DES UTILISATEURS

```
 DATA SECURITY-(CSECT1)- CERESSIA A.-

OBJECT CODE     ADDR1 ADDR2  STMT   SOURCE STATEMENT                                    ASM H V 05 19.51
                             241 ************************************************************************
                             242 *          * TABLE DES UTILISATEURS *                                  *
                             243 *          (EXEMPLE AVEC 10 ENTREES,8 UTIL.,5 GROUPES,24 BYTES(ENTREE) *
                             244 * REM:     (NOMBRE MININUM DE BYTES PAR ENTREE: 7)                     *
                             245 *           NI-MINIMUM 1BYTE,SOIT 255 NI POSSIBLES                     *
                             246 *           KEY-MINIMUM 4BYTES(PERD SON EFFICACITE SI ON LA REDUIT      *
                             247 *           RESPONSABLILITY- DE 0 A X BYTES(SI TROP GD,FAIRE UN FICHIER*
                             248 ************************************************************************
                             249            DS    0D
0001000A                     250 UTDEF      DC    H'1',H'10'                  NI 1 RESERVE/NBRE D'ENTR.
00000000                     251 GROUPE     DC    XL4'00'                     GR8    GR1  CADRAGE DROIT
0000001F                     252            DC    B'00000000000000000000000000011111'
0000000000000000             253            DC    12X'00'
0002C5E7C9E3F0F9             254 UT         DC    H'2',CL6'EXIT09',FL1'1',CL15'SECURITY OFFIC.'
0079C6D6D9D4F6F6             255            DC    H'121',CL6'FORM66',FL1'3',CL15'SYSTEMS ANALYST'
0225C6D3C1C7F3F3             256            DC    H'549',CL6'FLAG33',FL1'4',CL15'PROGRAMMER'
0400D7C5D9E2D6D5             257            DC    H'1024',CL6'PERSON',FL1'3',CL15'DP MANAGEMENT'
0800E2C8D6D7F1F0             258            DC    H'2048',CL6'SHOP10',FL1'4',CL15',PROGRAMMER'
09D9E2C5C1D9C3C8             259            DC    H'2521',CL6'SEARCH',FL1'5',CL15'OPERATOR'
0A3FE3C9D4C9D5C7             260            DC    H'2622',CL6'TIMING',FL1'3',CL15'SYSTEMS ANALYST'
0AB9C3C8C5C3D2F8             261            DC    H'2745',CL6'CHECK8',FL1'2',CL15'GENERAL MANAGT.'
0000404040404040             262            DC    H'0',6CL1' ',FL1'0',15CL1' '
0000404040404040             263            DC    H'0',6CL1' ',FL1'0',15CL1' '
                             264 END2       DS    0F
```


C
CSECTI
commande COPY ?
non
oui
copy
CSECT4
5
A
type de commande
insert
modify
delete
9
balayage de la table (calc. d'ad.)
SW2 à 0
SW2 à 1
IO
BALAYAGE DE LA TABLE
NI dans la table?
oui
non
"NI EXISTE DEJA"
clé identique ds la t. ?
non
oui
I3
"CLE existant déjà"
NI identique ds la t. ?
non
fin de table ?
non
IO
oui
SW2 ON ?
oui
II
SW2 ON ?
oui
SW2 à 0
non
"SUPPRES. D'UN UTIL. N'EXISTANT PAS"
"MODIFICAT. IMPOSSIBLE: UTIL. PAS DS LA TABLE"
Suppression: 0000 ds NI, b ds le reste
fin de table?
non
oui
"NOMBRE D'ENTREES INSUFFISANT"
nbre d'entrées libres >0
transfert des données dans une entrée
II
respons. clé
objet de la m. ?
NI
groupe
clé
clé ?
responsabilité
effectuer la modification
I2
balayage de la table
groupe existant?
non
oui
"GROUPE N'EXISTANT PAS DS GT"
I4
balayage de la table
NI identique ?
oui
clé identique ?
oui
I3
non
fin de table
I2
oui
non
I4
oui
"LE NI A MODIFIER N'EXISTE PAS"
effectuer la modification
C
4-I4

DATA SECURITY-(CSECT2)- CERESSIA A.-

TABLE DES GROUPES

```
OBJECT CODE     ADDR1 ADDR2  STMT   SOURCE STATEMENT                                                ASM H V 05 19.5
                             355 ************************************************************************************
                             356 *         TABLE DES GROUPES -48BYTES PAR ENTREE(JEU D'ESSAIS)
                             357 *         (EX. AVEC 10ENTREES,16PROG.,16FICHIERS POSSIBLES)
                             358 *
                             359 *         REM.: 16 BYTES(1 PAR PROGRAMME)     -CPP  MAXIMUM: 99
                             360 *               16*2 BYTES(2 PAR FICHIER)     -CE   MAXIMUM: 63
                             361 *                                             -CM   MAXIMUM:255
                             362 *               POUR CPP:(BIT 8 A 1)=STRATIFICATION (IDEM DS CE)
                             363 *               POUR CE: (BIT 7 A 1)=VIDAGE(AUTORISE)DU FICHIER
                             364 ************************************************************************************
                             365 *                    87654321 87654321 87654321 87654321      BIT ON=PRESENT
0000001F                     366 GT       DC      B'00000000 00000000 00000000 00011111'           GROUPES
0000420B                     367          DC      B'00000000 00000000 01000010 00001011'           PROGRAMMES
00000003                     368          DC      B'00000000 00000000 00000000 00000011'           FICHIERS
                             369 *                  *   RESERVES   **      TABLE   *
0005                         370 CPTG     DC      H'5'
0005                         371 CPTPRG   DC      H'5'
0002                         372 CPTFCH   DC      H'2'
                             373 *
0000000000000000             374 G1       DC      16X'00'
4101410141014101             375          DC      8XL2'4101'
4101410141014101             376          DC      8XL2'4101'
                             377 *
0101000100000000             378 G2       DC      2X'01',X'00',X'01',5X'00',X'01',4X'00',X'01',X'00'
0101050100010001             379          DC      2X'01',X'05',X'01',14XL2'0001'
                             380 *
0101000100000000             381 G3       DC      2X'01',X'00',X'01',5X'00',X'01',4X'00',X'01',X'00'
4202460200000000             382          DC      XL2'4202',XL2'4602',28X'00'
                             383 *
8381008400000000             384 G4       DC      XL2'8381',X'00',X'84',10X'00',X'86',X'00'
8404140500000000             385          DC      XL2'8404',XL2'1405',28X'00'
                             386 *                                                                    *
0001008500000000             387 G5       DC      XL4'00010085',12X'00'
8505000000000000             388          DC      XL4'85050000',28X'00'
                             389 *
0000000000000000             390 G6G10    DC      5XL48'00'
                             391 *
```

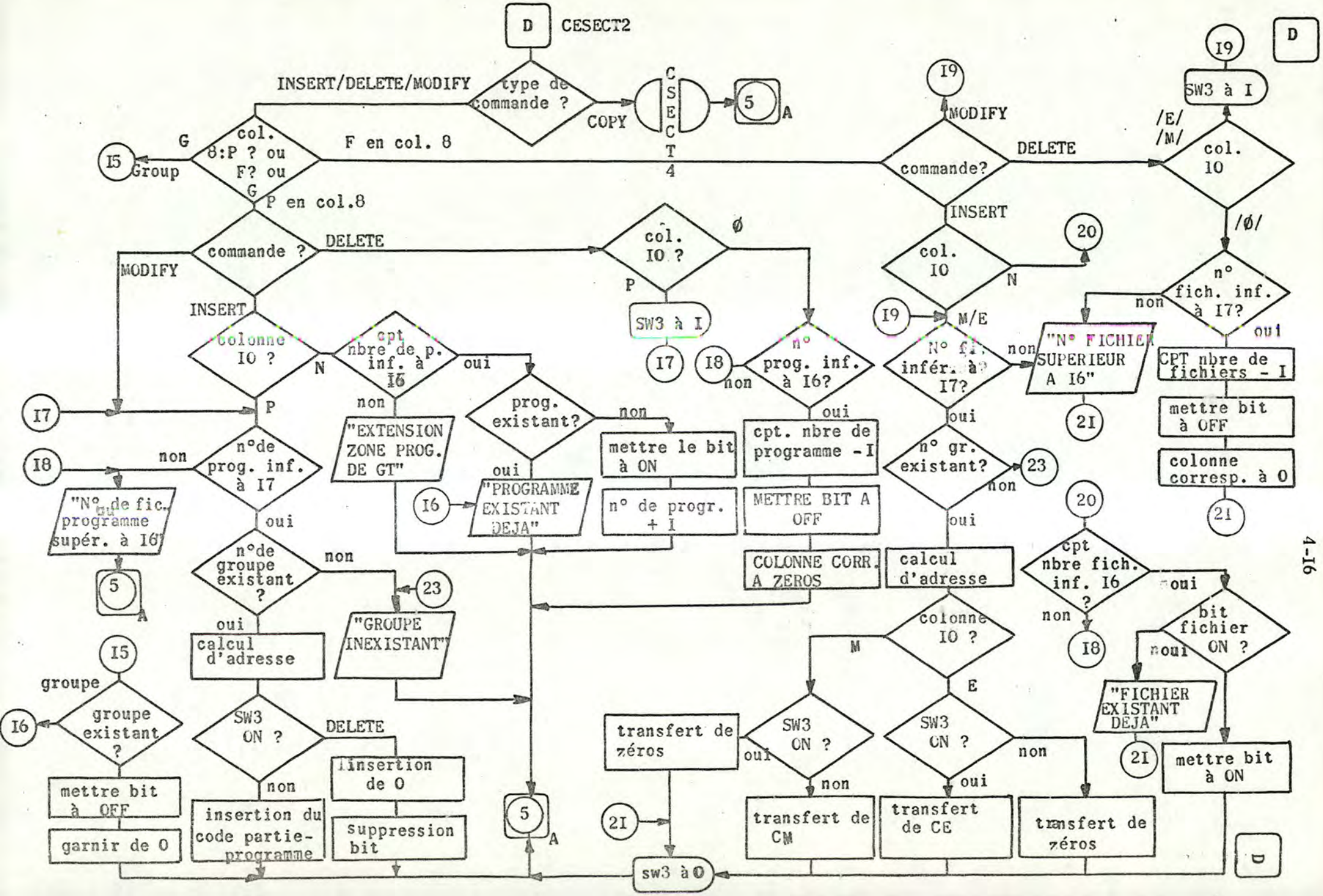
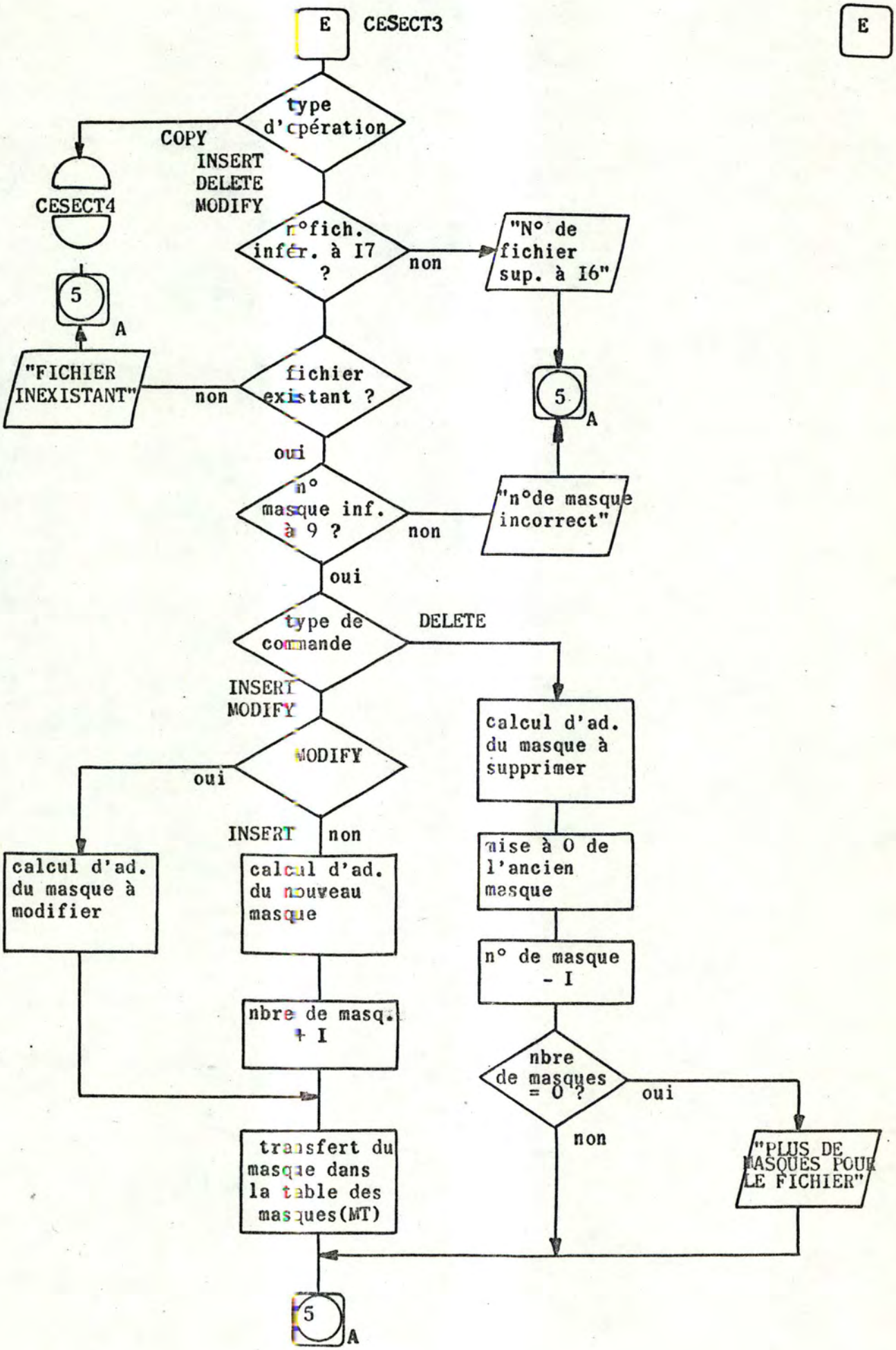
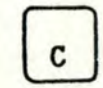

D
CESECT2
type de commande ?
INSERT/DELETE/MODIFY
COPY
CSECT 4
5 A
col. 8:P ? ou F? ou G
G
I5 Group
F en col. 8
P en col.8
commande ?
DELETE
MODIFY
INSERT
colonne IO ?
N
P
cpt nbre de p. inf. à I6
oui
non
"EXTENSION ZONE PROG. DE GT"
I7
I8
non
n°de prog. inf. à I7
"N° de fic. programme supér. à I6"
oui
n°de groupe existant ?
non
23
"GROUPE INEXISTANT"
oui
calcul d'adresse
SW3 ON ?
DELETE
non
insertion de 0
insertion du code partie-programme
suppression bit
I5
groupe
I6
groupe existant ?
mettre bit à OFF
garnir de 0
col. IO ?
Ø
P
SW3 à I
I7
I8
n° prog. inf. à I6?
non
oui
cpt. nbre de programme - I
METTRE BIT A OFF
COLONNE CORR. A ZEROS
prog. existant?
non
oui
mettre le bit à ON
n° de progr. + I
I6
"PROGRAMME EXISTANT DEJA"
5 A
I9
MODIFY
commande?
DELETE
INSERT
col. IO
N
20
I9
M/E
N° fich. inférieur à I7?
non
"N° FICHIER SUPERIEUR A I6"
21
oui
n° gr. existant?
23
non
oui
calcul d'adresse
colonne IO ?
M
E
SW3 ON ?
oui
non
transfert de zéros
transfert de CM
SW3 ON ?
oui
non
transfert de CE
transfert de zéros
21
sw3 à 0
I9
SW3 à I
/E/ /M/
col. IO
/Ø/
n° fich. inf. à I7?
non
oui
CPT nbre de fichiers - I
mettre bit à OFF
colonne corresp. à 0
21
20
cpt nbre fich. inf. I6 ?
non
oui
I8
bit fichier ON ?
oui
non
"FICHIER EXISTANT DEJA"
21
mettre bit à ON
D

TABLE DES MASQUES

```
202 ********************************************************************************
203 *                                                                              *
204 *         TABLE DES MASQUES DES FICHIERS                                       *
205 *         EXEMPLE:  ENTREE DE LONGUEUR FIXE = 53 BYTES                         *
206 *                     -NOMBRE MAX. DE MASQUES PAR FICHIER = 8                  *
207 *                     (TABLE DE BIT DE 1 BYTE- 1 BIT PAR MASQUE)               *
208 *                   NOMBRE MAX. D'ITEMS PAR ENREG. =16 (4BYTES/MASK)           *
209 *                     -FORMAT DE L'ENREGISTREMENT DU FICH.(16 BYTES)           *
210 *                     (LONG. TOTALE ET LONG. DE CHAQUE ITEM)                   *
211 *         REM.:     *LES ENREGISTREMENTS NE COMPORTERONT QUE DES CARAC.*
212 *                   POUR POUVOIR LES IMPRIMER DIRECTEMENT.EN PRATIQUE,*
213 *                   L'ENREGISTREMENT EST DESTINE AU PROGRAMME.                 *
214 *                                                                              *
215 *         CONVENTION:      MASK                                      ROOTS     *
216 *                     -00 PROTECTION                                 -PROTEC   *
217 *                     -01 WRITE ONLY                                 -WONLY    *
218 *                     -10 READ ONLY                                  -RONLY    *
219 *                     -11 READ/WRITE/UPDATE  (NO PROTECTION)         -RW       *
220 ********************************************************************************
221 *                FORMAT DE ZWORK5
222 *         ----------------------------------------------
223 MFILE1   DC     X'04'                    NBRE DE MASQUES PRES.(MAX.8)
224         DC     B'00011011'              TABLE DE BITS(MASK PRESENT)
225         DC     X'07'  (SS CLE ET CE)    NOMBRE D'ITEMS DANS L'ENREG.
226         DC     X'04'                    LONG. DU MASQUE(EN BYTES)
227         DC     X'3C'                    LONG. TOTALE(MAX 256)
228         DC     XL16'1405020101160500000000000000000'
229 *               ITEM  1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
230 *
231 *                  - - - - - - - - - - - - - - - -
232         DC     B'11111010101000000000000000000'          M1
233         DC     B'10101111111111000000000000000000'       M2
234         DC     B'00000000000000000000000000000000'       M3
235         DC     B'00001111111001000000000000000000'       M4
236         DC     B'00001010000000000000000000000000'       M5
237         DC     3XL4'00'                                  M6/7/8
238 *       ----------------------------------------------
239 MFILE2  DC     X'00'
240         DC     B'00000000'
241         DC     X'00'
242         DC     X'04'
243         DC     X'00'
244         DC     XL16'00'
245 *                  - - - - - - - - - - - - - - - -
246         DC     8XL4'00'
247 *       ----------------------------------------------
248 MFILE316 DC     14XL53'00'
249 ********************************************************************************
```


E
CESECT3
E
type d'opération
COPY
INSERT
DELETE
MODIFY
CESECT4
n°fich. infér. à I7 ?
non
"N° de fichier sup. à I6"
5
A
"FICHIER INEXISTANT"
non
fichier existant ?
5
A
oui
n° masque inf. à 9 ?
non
"n°de masque incorrect"
oui
type de commande
DELETE
INSERT
MODIFY
calcul d'ad. du masque à supprimer
MODIFY
oui
INSERT
non
calcul d'ad. du masque à modifier
calcul d'ad. du nouveau masque
mise à 0 de l'ancien masque
n° de masque - I
nbre de masq. + I
nbre de masques = 0 ?
oui
non
transfert du masque dans la table des masques(MT)
"PLUS DE MASQUES POUR LE FICHIER"
5
A

```
ADRESS A015
                                                TA A015    **TERMINAL ADRESS

>ENTER YOUR PERSONNEL NUMBER
LOGON     2

>ENTER YOUR KEY
KEY    EXIT09

>ENTER MESSAGE
C      /U/
***ERROR IN FUNCTION-IGNORED
                     -ENTRY TYPE IS INVALID OR
                     -INVALID POSITIONAL PARAMETER

>ENTER MESSAGE
COPY   /U
***ERROR IN FUNCTION-IGNORED
                     -ENTRY TYPE IS INVALID OR
                     -INVALID POSITIONAL PARAMETER

>ENTER MESSAGE
COP    /U/
***ERROR IN FUNCTION-IGNORED
                     -ENTRY TYPE IS INVALID OR
                     -INVALID POSITIONAL PARAMETER

>ENTER MESSAGE
COPY   /T/
***ERROR IN FUNCTION-IGNORED
                     -ENTRY TYPE IS INVALID OR
                     -INVALID POSITIONAL PARAMETER

>ENTER MESSAGE
COPY   /U/
                     * TABLE DES UTILISATEURS *

      NI     KEY   GR   RESPONSABILITY
     ------------------------------------
      0002 EXIT09 01 SECURITY OFFIC.

      0121 FORM66 03 SYSTEMS ANALYST

      0549 FLAG33 04 PROGRAMMER

      1024 PERSON 03 DP MANAGEMENT

      2048 SHOP10 04 ,PROGRAMMER

      2521 SEARCH 05 OPERATOR

      2622 TIMING 03 STSTEMS ANALYST

      2745 CHECK8 02 GENERAL MANAGT.
>ENTER MESSAGE
DELETE/U/0560
***ERROR IN FUNCTION-IGNORED
                     -INVALID POSITIONAL PARAMETER
     ERR2B-SUPPR. IMPOSSIBLE-UT.PAS DS UT

>ENTER MESSAGE
DELETE/U/1024
     PROCESSING COMPLETE:FUNCTION TERMINATED
```



```
>ENTER MESSAGE
MODIFY/U/0122,N,2525
***ERROR IN FUNCTION-IGNORED
                    -INVALID POSITIONAL PARAMETER
     ERR3B-MODIF. IMPOSSIBLE-UT.PAS DS UT

>ENTER MESSAGE
MODIFY/U/0121,N,2525
     PROCESSING COMPLETE:FUNCTION TERMINATED

>ENTER MESSAGE
MODIFY/U/2525,K,STACK1
     PROCESSING COMPLETE:FUNCTION TERMINATED

>ENTER MESSAGE
MODIFY/U/2525,G,06
***ERROR IN FUNCTION-IGNORED
                    -INVALID POSITIONAL PARAMETER
     ERR3G-MOD. IMP.-GR. INEXISTANT

>ENTER MESSAGE
MODIFY/U/2525,R,ASSISTANT
     PROCESSING COMPLETE:FUNCTION TERMINATED

>ENTER MESSAGE
INSERT/U/0122FORM4405EMPLOYEE
     PROCESSING COMPLETE:FUNCTION TERMINATED

>ENTER MESSAGE
MODIFY/U/0549,N,0549
     PROCESSING COMPLETE:FUNCTION TERMINATED

>ENTER MESSAGE
COPY  /U/
                    * TABLE DES UTILISATEURS *
      NI    KEY   GR  RESPONSABILITY
     ------------------------------------
     0002 EXIT09 01 SECURITY OFFIC.

     2525 STACK1 03 ASSISTANT

     0549 FLAG33 04 PROGRAMMER

     0000        00

     2048 SHOP10 04 ,PROGRAMMER

     2521 SEARCH 05 OPERATOR

     2622 TIMING 03 SYSTEMS ANALYST

     2745 CHECK8 02 GENERAL MANAGT.

     0000        00

     0122 FORM44 05 EMPLOYEE

     PROCESSING COMPLETE:FUNCTION TERMINATED
```

```
>ENTER MESSAGE
COPY  /G/
     PROCESSING COMPLETE:FUNCTION TERMINATED

>ENTER MESSAGE
INSERT/P/N/25
***ERROR IN FUNCTION-IGNORED
                    -INVALID POSITIONAL PARAMETER
     ERR.9A/6A/11A-NP N'EXISTANT PAS

>ENTER MESSAGE
INSERT/P/N/08
     PROCESSING COMPLETE:FUNCTION TERMINATED

>ENTER MESSAGE
INSERT/F/N/03
     PROCESSING COMPLETE:FUNCTION TERMINATED

>ENTER MESSAGE
INSERT/P/P/02,08,01
     PROCESSING COMPLETE:FUNCTION TERMINATED

>ENTER MESSAGE
INSERT/F/E/02,03,005
     PROCESSING COMPLETE:FUNCTION TERMINATED

>ENTER MESSAGE
INSERT/F/M/10,03,02
***ERROR IN FUNCTION-IGNORED
                    -INVALID POSITIONAL PARAMETER
     ERR.9B/12B/14B/18A-GR.N'EXISTANT PAS

>ENTER MESSAGE
INSERT/F/M/02,03,02
     PROCESSING COMPLETE:FUNCTION TERMINATED
>ENTER MESSAGE
COPY  /G/
     PROCESSING COMPLETE:FUNCTION TERMINATED
```

D

```
>ENTER MESSAGE
COPY  /M/
     PROCESSING COMPLETE:FUNCTION TERMINATED

>ENTER MESSAGE
INSERT/M/01,08,00010101101000010000000000000000'
     PROCESSING COMPLETE:FUNCTION TERMINATED

>ENTER MESSAGE
DELETE/M/01,02
     PROCESSING COMPLETE:FUNCTION TERMINATED

>ENTER MESSAGE
MODIFY/M/01,08,00011000000000000000000000000000'
     PROCESSING COMPLETE:FUNCTION TERMINATED

>ENTER MESSAGE
COPY  /M/
     PROCESSING COMPLETE:FUNCTION TERMINATED

>ENTER MESSAGE
LOGOFF
```

E

CHAPITRE 5:
conclusions

"Les erreurs accidentelles et délibérées ne sont pas spécifiques des systèmes informatiques et les organisations manuelles étaient et restent tout aussi vulnérables si ce n'est plus, car je suis assez tenté de croire que l'informatique est mieux armée pour faire face à ces dangers, à condition de vouloir et de savoir y faire face".

(SLIGOS INTERFACE IC/74)

Gérard BAUVIN

Si d'une part, les progrès de l'informatique dans des domaines comme les bases de données ou les réseaux de communications et, d'autre part, le développement de la criminalité par l'informatique, ont contribués à la prise en considération actuelle par les utilisateurs et constructeurs des problèmes liés à la sécurité des données, il n'en reste pas moins vrai, qu'actuellement, très peu de systèmes de gestion de bases de données offrent une solution globale et efficace.

Beaucoup de constructeurs se sont limités aux dispositifs de protection existant dans leur système d'exploitation (protection mémoire, label disque et bande, isolation des programmes dans les systèmes avec multiprogrammation....) et ne se sont pas penchés davantage sur le problème lors de la conception de leur système de gestion de bases de données.

Les utilisateurs, quant à eux, n'ont été vraiment sensibilisés aux problèmes de sécurité que depuis la création de vastes bases de données où des informations n'exigeant aucune protection cotoient des informations sur leur vie privée ou sur des secrets commerciaux (fichiers marketing, clients, crédits accordés aux clients ou accordés par les fournisseurs...)

Bien que le problème des banques de données sur la vie privée des individus ait soulevé de nombreuses discussions (ces dernières entraînant de nombreux projets de lois), il semble vraisemblablement qu'il faille atteindre un compromis de ce genre : soit que nous consentions à abandonner une partie du droit de préservation de notre vie privée (droit qui nous est propre depuis des siècles) ou soit que nous renoncions à certains avantages de notre société technologique.

Les nouveaux problèmes soulevés par la technologie montrent l'insuffisance et l'imperfection ces lois en vigueur. En fait, la technologie n'a pas nui au secret ou à la confidentialité des données, mais en a plutôt précipité l'aboutissement critique.

En tant que professionnels de l'informatique, nous avons la responsabilité d'avertir les utilisateurs et le public des systèmes de sécurité qui peuvent être élaborés dans le cas des ordinateurs fonctionnant en télétraitement, ainsi que des moyens de protection qui peuvent être mis en place.

A l'heure où l'on attend le vote de la loi sur le Registre National et sur la Protection des Libertés Individuelles, cette étude vient à point pour fournir aux responsables de réseaux de télétraitement un éventail des dispositifs de protection actuels ainsi qu'une méthodologie de mise en place d'un système de sécurité se servant de ceux-ci.

ANNEXES:

REALISATIONS ACTUELLES

annexe A: recommandations du Codasyl.

AI. AVANT-PROPOS : SGBD, INFLUENCES ACTUELLES.

Si on examine les différents softwares de gestion de bases de données proposés par les constructeurs et les sociétés de services actuels, il semble qu'il y ait, en première approximation, trois influences :

- IBM (IMS) ;
- les travaux du DBTG (Data Base Task Group)du Codasyl ;
- les"autres" (parfois très importantes)

a) influence IBM :

- refuse les recommandations du DBTG,
- conception particulière (pas de notions de Schéma et Sous-Schémas)
  (remarque : le début des travaux communs IBM/North American Rockwell sur IMS remonte à près de dix ans et est donc bien antérieur au rapport du DBTG d'octobre 69)
- Système de gestion de BD : IMS (voir annexe B I)

b) influence DBTG :

- Systèmes de gestion de bases de données conformes aux recommandations du DBTG :
- Exemples : - chez UNIVAC :
  .DMS 1100 (pour la série 1100)
  .DMS 90 (opérationnel sur 90/60 et 90/70 ØS7)
  - PHILIPS (et UNIDATA) :
  .PHOLAS
  - METRA INTERNATIONAL(GOODRICH CHEMINAL Co) :
  .IDMS
  - HONEYWELL BULL :
  .IDS (bien que très antérieur aux travaux du DBTG, il semble s'en rapprocher de plus en plus (voir annexe B2

c) les "autres" :

- CII : SOCRATE : (offre un langage autonome, à la différence d'autres systèmes qui utilisent un langage hôte.)

- Burroughs : FORTE : (présente une caractéristique originale : les Tag et Bit Vectors - technique qui associe à un fichier de données, un fichier de caractéristiques (le Bit Vector) converties en binaire ; ce fichier permet ensuite d'effectuer sur le fichier "source" des recherches sélectives très rapides en remontant du Bit Vector aux enregistrements recherchés.

Remarquons que d'autres organismes que le DBTG tels que Club Banque de données de l'IRIA, JOINT GUIDE/SHARE DATA BASE REQUIREMENTS GROUP) ont entrepris, depuis plusieurs années, de définir de manière précise les objectifs d'un SGBD ainsi que les spécifications qui en découlent. Si actuellement les constructeurs se sentent surtout concernés par les travaux de CODASYL, rien ne permet cependant de penser qu'il puisse se créer à court terme une unité comparable à celle qui s'est faite notamment autour des langages.

A.2 RECOMMANDATIONS DU DBTG CONCERNANT LA CONFIDENTIALITE ET L'INTEGRITE DES DONNEES.

Ces recommandations portent d'une part :

- sur la protection de la confidentialité en cas d'accès non autorisés aux données,
  (permet de régler les problèmes de protection des données confidentielles d'un fichier personnel, clients, marketing, etc..);

et d'autre part :

- sur la sauvegarde de l'intégrité des données lors d'interférences entre programmes ;
  (permet de régler les problèmes de concurrence entre programmes).

A.2.I PROTECTION DE LA CONFIDENTIALITE

1. Définition de serrures (PRIVACY LOCKS) :

   .Peuvent être définies à six niveaux différents allant de la base de données aux items.

   .Spécifiées au moyen d'instructions du DML (data manipulation langage).

2. Utilisation de clés (PRIVACY KEYS) :

   .Fournies par le programmeur lorsqu'il veut accéder ou modifier des données protégées par des privacy locks.

   exemple : pour un record : lors des instructions INSERT, STORE, MODIFY, DELETE, GET et FIND ;

   pour un item : lors des instructions GET, MODIFY et STORE ;

   pour des relations entre records : lors des instructions ORDER, FIND, REMOVE et INSERT.

   .Spécifiées en "identification division" du programme en langage hôte ;

   .Fournies sous la forme soit :

- d'un littéral,
- d'un nom d'item situé dans la zone de travail de l'utilisateur (UWA)
- d'un nom de procédure (sera chargée de générer la clé nécessaire.

3. Utilisation d'une procédure jouant le rôle de "privacy lock" :

elle permettra par exemple,
. de valider une "privacy key",
. de poser des questions à l'utilisateur du terminal (procédure d'identification - voir chap. II : 5.2.2.)
. d'arrêter un processus en cas de tentatives de violation répétées,
. de déconnecter le terminal.

A.2.2 SAUVEGARDE DE L'INTEGRITE

I. Principe de base :

. le système n'exécute pas l'instruction de modification qui suit un FIND (détermination de l'occurence du record) si un programme concurrent a exécuté entretemps une modification autorisée sur le même record ;

. a ce moment, le prgramme en cours d'exécution peut choisir entre d'une part,

- exécuter sa modification sans tenir compte de celle faite éventuellement par un programme concurrent,

d'autre part,

- réaccéder à l'enregistrement éventuellement modifié par un programme concurrent et donc tenir compte de la modification.

. exemple : tentative pour effectuer une balance de vérification alors que des transactions affectant les différents postes des comptes sont encore en cours de réalisation.

2. Fonctionnement :

.Chaque programme peut obtenir, lors de l'instruction OPEN, le contrôle exclusif ou protégé d'une ou plusieurs "areas" (concept de fichier). Il perdra ce contrôle lors de l'instruction CLOSE ou lors d'une fin anormale (cas d'une tentative de violation répétée).

- clause "EXCLUSIVE" dans l'ordre OPEN :

.empêche toute interférence, quel que soit le mode d'accès (usage-mode), entre deux programmes concurrents s'adressant à la même "area".

exemple : la figure suivante représente les oppositions de mode d'accès entre deux programmes essayant d'exécuter un ordre OPEN sur la même "area".

	6	7	5	4	3	2	I
I. ni lecture ni écriture	X	X	OK	OK	OK	OK	OK
2. lecture	X	X	OK	OK	OK	OK	
3. mise à jour	X	X	X	X	OK		
4. lecture protégée	X	X	X	OK			
5. mise à jour protégée	X	X	X				
6. lecture exclusive	X	X					
7. mise à jour exclusive	X						

(X indique une opposition entre les modes d'accès indiqués dans les deux programmes).

- clause "PROTECTED" dans l'ordre OPEN :

  .empêche les mises à jour concurrentes ;

  . permet les lectures concurrentes dans la même "area"

  .clause moins restrictive que la précédente.

3. remarque :

.Les options "EXCLUSIVE" et "PROTECTED de la commande OPEN ne permettent pas de résoudre le problème des interblocages (deadlock). Celui-ci est laissé à l'implémenteur.

exemple d'interblocage : soit deux programmes A et B et deux "areas" X (sous le contrôle exclusif de A) et Y (sous le contrôle exclusif de B). On aura un interblocage si les programmes veulent simultanément faire un OPEN de l'area qui n'est pas sous son usage exclusif.

annexe b: securité des données.

BI. SECURITE DES DONNEES EN IMS/VS (IBM)

BI. I INTRODUCTION

IMS/VS permet d'étendre les possibilités du système d'exploitation avec mémoire virtuelle, OS/VS, à un environnement base de données et communication de données.

Des terminaux permettent aux utilisateurs d'accéder à partir de leur département à la même base de données. Un contrôle rigoureux sera donc nécessaire. Un même terminal peut être utilisé pour une ou plusieurs applications.
IMS/VS peut recevoir et transmettre de nombreux types de messages se référant à des applications écrites (par l'utilisateur) en Assembler, Cobol ou PL/I. Celle-ci seront orientées batch ou télétraitement. Dans ce dernier cas, l'utilisateur devra écrire des programmes d'application qui contrôleront d'une part, la transmission de messages vers ou à partir des terminaux, et d'autre part, l'accès à la base de données. IMS supporte des opérations concurrentes venant de plusieurs programmes.

BI. 2 STRUCTURE DU SYSTEME IMS/VS

IMS/VS englobe trois grandes parties fonctionnelles ; les deux premières constituent un ensemble de fonctions liées à la base de données ou au système de communication de données, la troisième partie comprend un ensemble de programmes utilitaires.

BI.2.I LANGAGE ASSOCIE A LA BASE DE DONNEES.

DATA LANGUAGE/I permet la définition, la création, l'accès et la maintenance de la base de données.
Un programme d'application a deux interfaces distincts avec DL/I :

a) une description de la base de données :
   c'est-à-dire la structure logique des données de la base, fournie comme une définition externe au programme d'application.

b) un relieur de programmes :
   permet au DL/I de traiter les demandes d'entrées/sorties durant l'exécution du programme d'application.

Dans un complexe télétraitement, DL/I fournit de plus,

un interface pour l'entrée et la sortie des messages des terminaux.

BI.2.2 DISPOSITIF DE COMMUNICATION DE DONNEES.

Celui-ci comprend les parties :

- TELECOMMUNICATIONS

la partie télécommunication constitue l'interface entre les terminaux de communication et le reste du système IMS ; elle fournit des fonctions telles que :

. l'initiation et le contrôle de toutes les opérations (I/O) sur les lignes ;

. la mise en file d'attente des messages d'entrée et de sortie sur une mémoire à accès direct.

Suivant les objectifs de chaque application, les messages en provenance des terminaux seront envoyés soit vers un programme d'application qui assurera leur traitement, soit vers un autre terminal. (Commutation de messages).

- ORDONNANCEMENT DES MESSAGES

IMS/VS assure :

. la prise en charge des messages ;

. l'initialisation des programmes de traitement d'après le type de message reçu ;

. le placement du message (d'après les attributs associés à la transaction), s'il est valide (après analyse du type de message), dans la file d'attente des messages prêts à être traités;

. initialisation du traitement dès que les ressources sont disponibles.

- PRISE DE POINT DE CONTROLE (OU CHECKPOINT).

Voir paragraphe BI.4.6.

- FONCTION DE REPRISE (OU RESTART

Voir paragraphe BI.4.6.

BI.2.3 PROGRAMMES UTILITAIRES.

Ces programmes sont destinés à assurer :

- la définition du système au moyen de blocs de contrôle ;
- la génération des blocs de contrôle décrivant la base de données, (voir Fig. B.8) ;
- la génération du PSB (Program Specification Block) associé à chaque programme. (voir Fig. B.6) ;
- la maintenance des blocs de contrôle associés aux applications ;
- le chargement, la réorganisation, le vidage et le recouvrement de la base de données, (voir Fig. B.I) ;
- l'analyse d'enregistrements statistiques concernant les types de messages et les commandes entrées aux terminaux ;
- le formattage des messages associés aux terminaux de display au moyen d'un langage de définition de formats.

BI. 3 DIAGRAMME DES FLUX D'INFORMATIONS. (voir Fig. BI)

Après la phase d'initialisation (exécutée par les programmes du job management du système d'exploitation) de la région ou partition A contenant le programme de contrôle IMS/VS et d'une ou plusieurs régions ou partitions utilisées pour le traitement des messages, les flux d'informations s'établissent comme suit :

1. Le dispositif de télécommunication demande des instructions de démarrage au terminal principal. (I). Une fois la procédure exécutée, celui-ci permet à tous les terminaux d'entrer en communication avec le système (2).
2. Dès la réception d'un message d'entrée, le dispositif de télécommunication passe le contrôle à un ensemble de programmes de services (3). Ceux-ci vont :
   - stocker le message sur une bande de sauvetage
   - et le placer dans la file d'attente des messages prêts à être exécutés (5).
3. Lorsque toutes les ressources nécessaires à son traitement seront disponibles, le dispositif d'ordonnancement déterminera le programme d'application qui sera chargé dans la région ou partition B et qui recevra le contrôle.
4. Les programmes du DL/I constitueront l'interface de contrôle (voir Fig. BI, B4 et B5) entre d'une part, le programme d'application (6) et d'autre part ; soit :

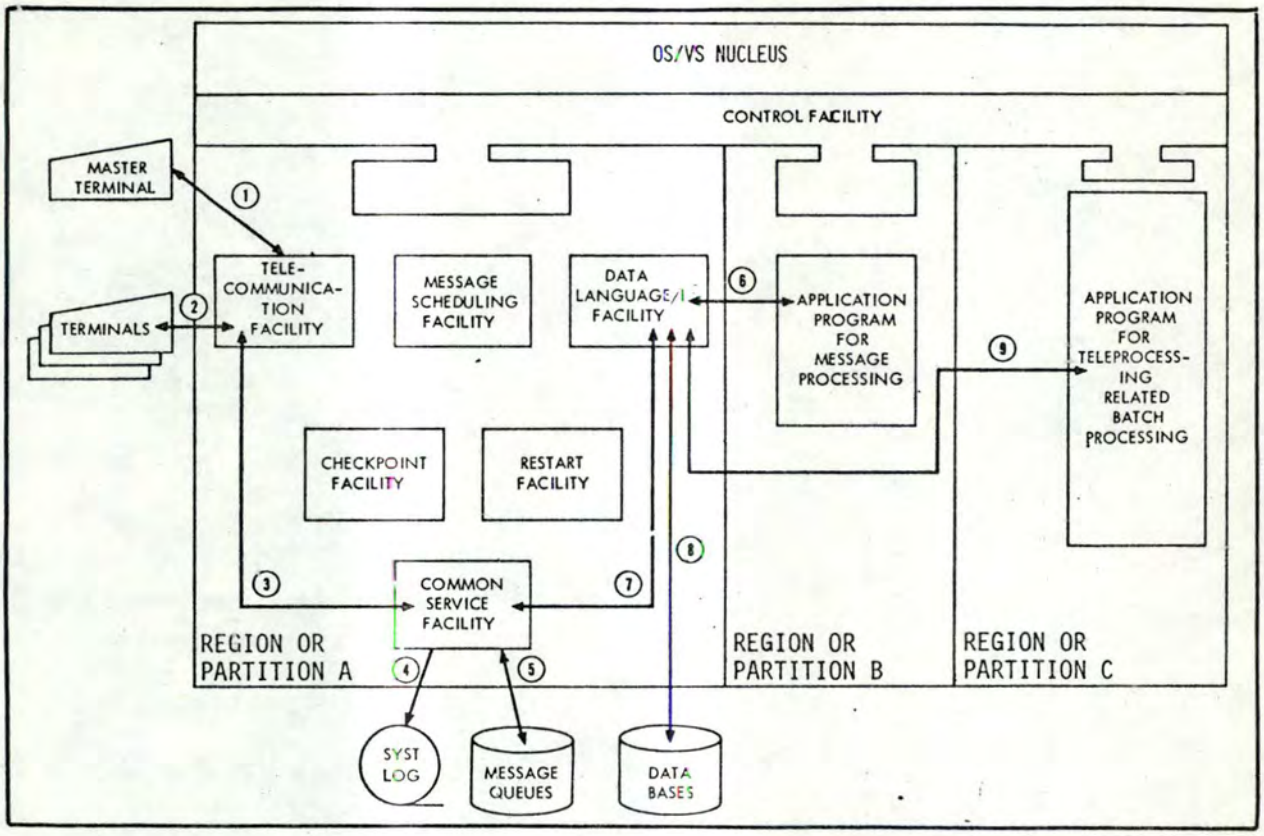


fig. BI_a

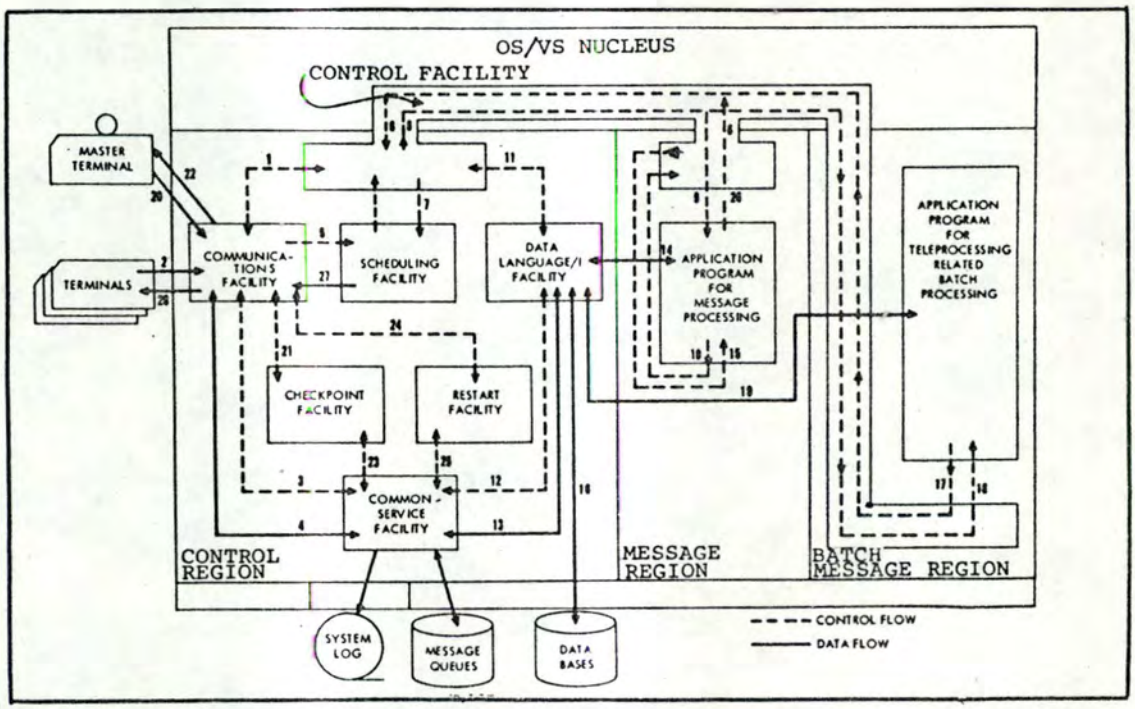


fig. BI_b

. le dispositif d'entrée de messages lors de la prise en charge d'un message prêt à être exécuté (7) ;

. la base de données lors d'une demande de données (8).

5. L'exécution d'un programme d'application entraîne :

. une éventuelle modification de la base de données (8) ;

. une mise en file d'attente de messages de sortie : (7 et 5).

6. Lorsqu'un programme d'application se termine ou demande un autre message en entrée, l'ensemble des messages de sortie, situés dans la file d'attente, sont transmis vers les terminaux correspondants.

7. Une région ou partition C déstinée au programme BATCH peut également être initialisée par le Job Management. Comme ces programmes peuvent avoir accès à la base de données (8), il peut y avoir, à certains moments, une concurrence entre programmes BATCH et TELEPROCESSING (6 et 9)/

BI. 4 FONCTIONS D'IMS ASSURANT LA SECURITE DES DONNEES.

Etant donné qu'il constitue l'interface entre les utilisateurs et la base de données, il se doit d'avoir un ensemble de dispositifs d'identification et d'autorisation pour contrôler l'accès aux différentes informations (données, programmes) du système, ainsi que des dispositifs pour assurer l'intégrité de la base de données.

A. Au niveau du contrôle d'accès, on peut considérer deux fonctions primordiales :

. la fonction d'identification - du terminal
- de l'utilisateur

. la fonction d'autorisation : elle contrôle l'autorisation d'accès à toutes les données accessibles au système IMS ; celles-ci comprennent :

- la base de données ;
- les programmes d'application ;
- les utilitaires ;
- les tables, (blocs de contrôle) ;
- les terminaux.

B. Parallèlement à ces fonctions assurant la protection des données, six autres fonctions contribuent à la maintenance de l'intégrité de la base de données :

. fonction d'intégrité proprement dite ;

. journalisation et constitution en temps réel de données de contrôle (LOGGING ou archivage) ;

. administration
  - administrateur de la base de données,
  - administrateur de la communication des données ;

. procédure de rattrapage (back-up) et de recouvrement (RECOVERY) ;

. point de contrôle et de reprise (CHECPOINT/REST.);

. vérification, contrôle et constitution de statistiques (auditings aids).

BI.4.I. IDENTIFICATION

A. Terminal logique et physique

- l'identification d'un utilisateur à un terminal nous oblige à faire la distinction entre les terminaux reliés au système au moyen :

  . d'une ligne louée : (Fig. B2a)

    IMS/VS connait depuis la définition du système le terminal qui lui est relié ainsi que les codes transaction et les mots de passe associés à celui-ci.

  . d'une ligne commutée (Fig. B2b)

    L'utilisateur doit s'identifier lui-même au moyen de la commande /IAM afin de permettre au système de le reconnaître et de lui assigner la liste des codes transaction qu'il est susceptible d'utiliser. La commande d'identification permet, en fait, d'établir la relation entre le nom d'un terminal logique (avec sa liste de code) et un terminal physique. (Fig. B2c)

    A un moment donné, un terminal physique n'est connecté qu'à un seul terminal logique.

- Dès cet instant, la procédure est identique dans les deux cas.

B. Introduction d'une transaction

- Chaque utilisateur (directeur général, chef de service, employé) doit introduire le code transaction identifiant la transaction qu'il veut exécuter;

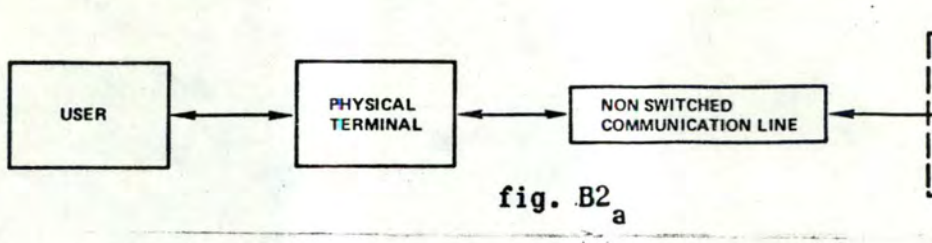


fig. $B2_a$

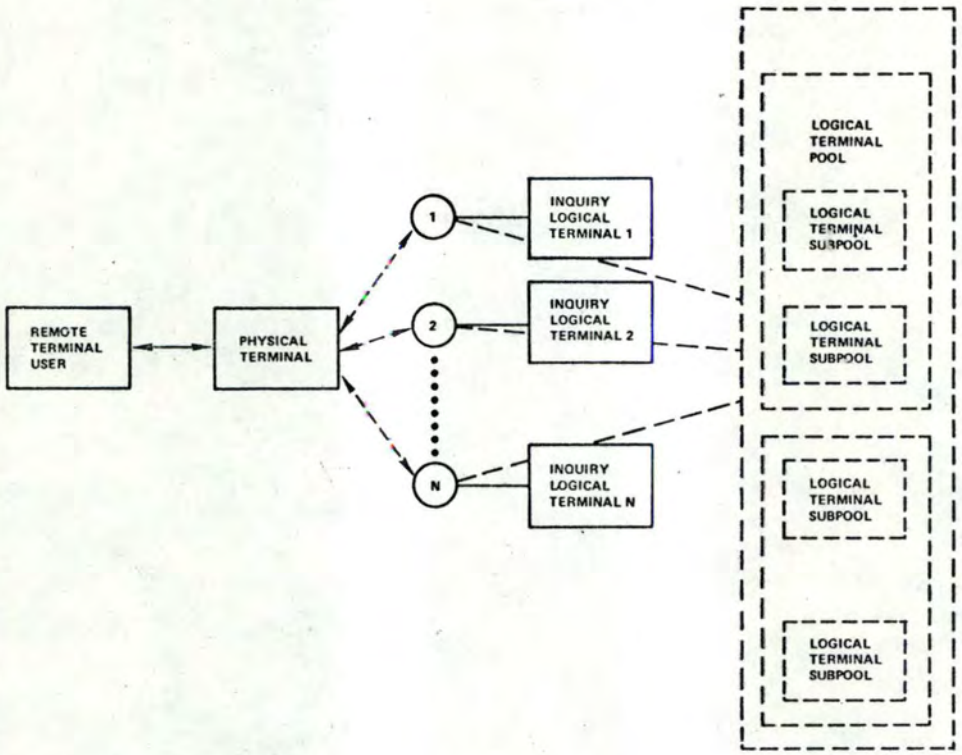


fig. $B2_b$

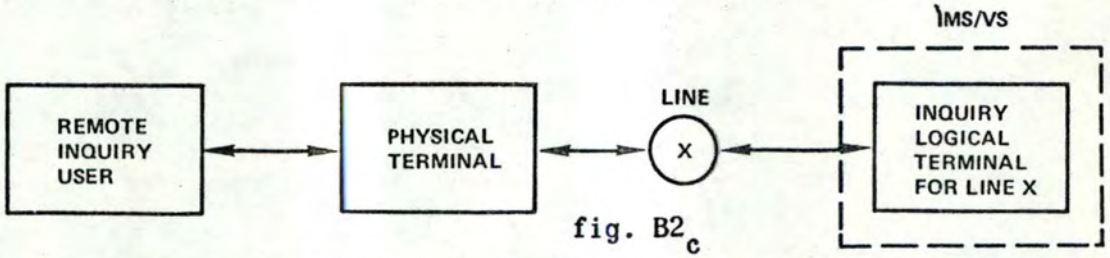


fig. $B2_c$

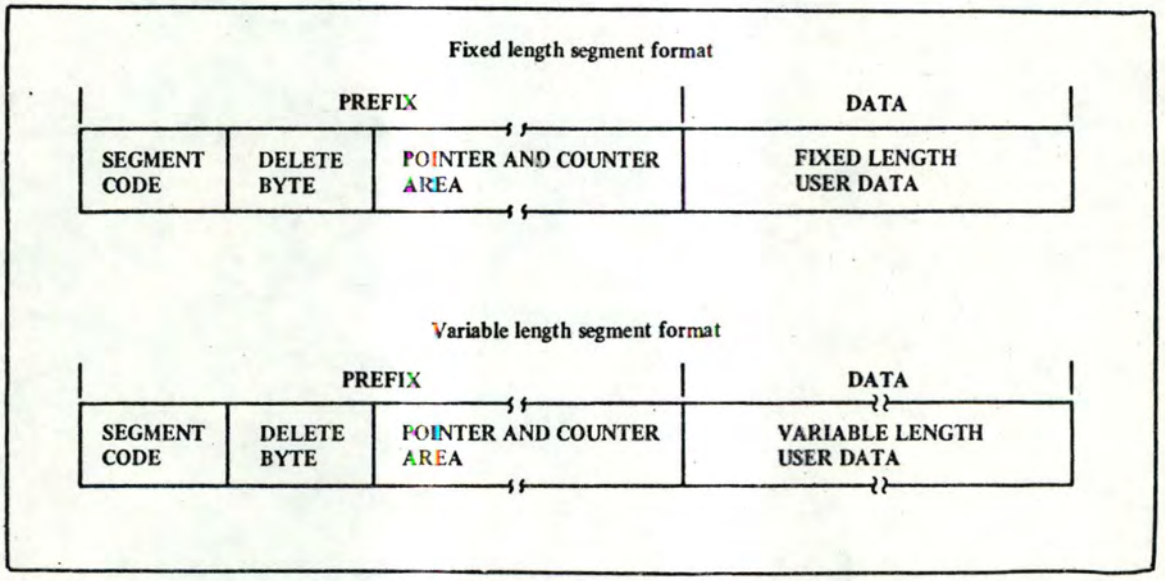


fig. B_3

Un même code peut être assigné à plusieurs terminaux logiques ce qui permet à tous les utilisateurs d'un même département, (ex : employés du service financier) d'utiliser le même code transaction et donc d'avoir accès au même programme qui traitera cette transaction. IMS/VS donne la possibilité de brancher à une routine permettant d'identifier l'utilisateur de manière univoque sur base de caractéristiques personnelles.

- Le mot de passe devra également être introduit si l'installation en a assigné un à cette transaction ; par code transaction, un seul mot de passe est admis. Dans le cas contraire, la transaction sera rejetée .

- Remarque : . Chaque paire (code transaction/mot de passe se retrouvera dans la liste associée à chaque terminal logique pouvant accepter cette transaction (voir Fig. $B2_b$).
  L'utilisateur peut obtenir la liste des codes transaction mais pas les mots de passe qui y sont associés.

C. Introduction d'une commande

- Dans une installation complexe désservant de nombreux utilisateurs et applications, il est nécessaire de pouvoir disposer d'un ensemble de commandes permettant d'agir sur le système à partir des terminaux. Chaque commande exécute une fonction séparée.

  . Exemples : /IAM, /LOG, /LOCK, /RDISPLAY...

- Celles-ci s'adressent à la base de données, aux terminaux ou aux programmes. On peut restreindre leur emploi à certaines personnes autorisées :

  . si la commande ne peut être entrée qu'à partir de certains terminaux (ex : ceux du service administratif) ;
  . si un mot de passe doit être introduit avec la clé ;
  . si on combine les deux possibilités précédentes.

BI.4.2. AUTORISATION

BI.4.2.1. PLAN D'AUTORISATION ET PROGRAMME DE MAINTENANCE DE LA SECURITE.

Pour assurer un meilleur contrôle de l'assignation de mots de passe aux codes transaction et aux commandes, une installation peut concevoir et implémenter un plan d'autorisation (AUTHORIZATION PLAN) reprenant ces assignations et la façon de les définir.

IMS/VS réalise ce plan au moyen d'un programme spécial de maintenance de la sécurité (SECURITY MAINTENANCE PROGRAM), qui a pour rôle de :

. créer les mots de passe associés aux
  - transactions;
  - commandes ;
  - programmes ;
  - bases de données ;

. modifier toutes informations concernant la sécurité, sans devoir redéfinir tout le système.

BI.4.2.2. ACCES A LA BASE DE DONNEES, BLOCS (TABLES)DE SPECIFICATIONS

Si le code entré par l'utilisateur a été défini comme un code transaction, le message sera envoyé vers un programme d'application.

Chaque transaction, donc chaque programme, n'aura accès qu'aux fichiers (concept d'AREA de CODASYL) de données autorisés par le PSB (PROGRAM SPECIFICATION BLOCK) et le DBD (DATA BASE DESCRIPTION BLOCK)-(semblable au concept de SUB-SCHEMA de CODASYL). Ces blocs sont simplement des tables qui sont examinées à chaque demande d'accès. (voir FIg. B6 et B8)

Le système identifie chaque programme au moyen de son PSBNAME, auquel est associé un ou plusieurs codes transaction: (rappelons que le code transaction permet à l'utilisateur de fournir au système un moyen d'identification du programme à exécuter)

. le PSB connait les segments disponibles à chaque TRANSACTION.

- Un segment est un ensemble de données élémentaires formant un ensemble logique (concept d'enregistrement.)
- En IMS/VS une base de données se représente par une structure de segments dépendants l'un de l'autre. (voir Fig.B6 et B8).

. le système IMS connait donc, par l'intermédiaire du PSB, quelles sont les données autorisées à l'utilisateur ; ce sont les seules accessibles au programme.

. le PSB est généré par l'administrateur de la base de données à l'aide d'un macro-langage et remis aux programmeurs de l'application, ce qui leur permet de savoir à quels types de segments ils ont accès. (voir Fig. B6 : paramètre PRØCØPT de SENSEG)

Mode d'accès

Suivant l'application, une décision va être prise pour chaque type de segment ;

. actions de base :
- aucun accès : accès interdit à ce type de segment,
- lecture uniquement :(soit concurremment avec d'autres utilisateurs soit exclusivement.)

. actions combinées avec une lecture :
- ajoute d'une nouvelle occurence de ce type de segment,
- mise à jour,
- suppression.

Remarque : Bien que l'autorisation d'accès soit déclarée au niveau du programme, si l'on combine ces possibilités avec un emploi judicieux des codes transaction et des mots de passe, IMS/VS fournit jusqu'a II niveaux de sécurité différents. Il est alors impossible de contrôler l'accès au niveau d'un segment individuel.

. exemple : si chaque code transaction est associé à un seul programme, l'autorisation d'accès sera déclarée au niveau de la transaction.

BI.4.2.3. REMARQUE : GENERATION DU PSB .

Avant qu'un programme d'application puisse être exécuté sous IMS/VS, il est nécessaire de décrire ce programme ainsi que ses besoins (nombre de terminaux logiques, hiérarchies de segments) en générant un PSB. (voir exemple de génération à la Fig. B6).

La décomposition d'un PSB fait apparaître un ou plusieurs blocs de contrôle qui lui sont subordonnés (PCB : PROGRAM COMMUNICATION BLOCK).

Chaque PCB spécifie au moins : (voir Fig.B6)

- une base de données (nom du DBD associé à ce programme) ;
- une structure logique de segments (ensembles de segments reliés hiérarchiquement et relatifs à la B.D.)
- éventuellement d'autres paramètres.

La figure B5aindique les différentes librairies qui fourniront les éléments (programmesd'application, données, utilitaires, blocs de contrôle) nécessaires au traitement des transactions.

La figure B5b indique la séquence des opérations effectuées dans le cas d'une lecture et montre très clairement le rôle du DL/I.

BI.4.2.4. CONCLUSIONS.

La plus petite unité d'information pouvant être protégée en IMS/VS est le segment.

Remarque : A l'intérieur du segment, il est possible d'encoder/décoder les données au moyen de routines de compaction (SCRAMBLING ROUTINES) écrites par l'utilisateur (voir chapitre II ; section 7, techniques cryptographiques).

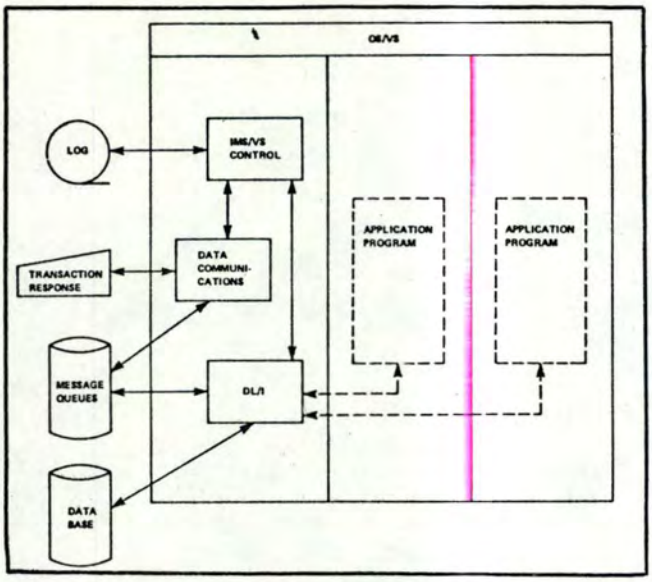


fig. B_4

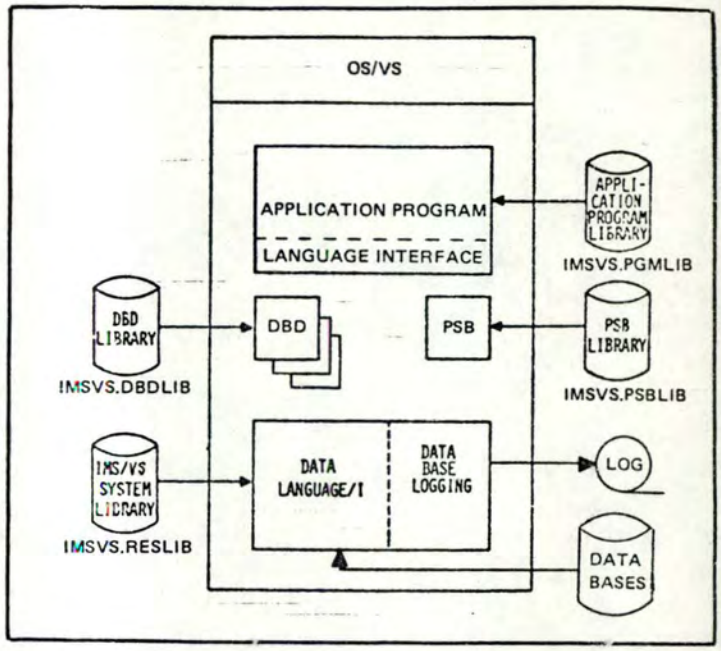


fig. $B5_a$

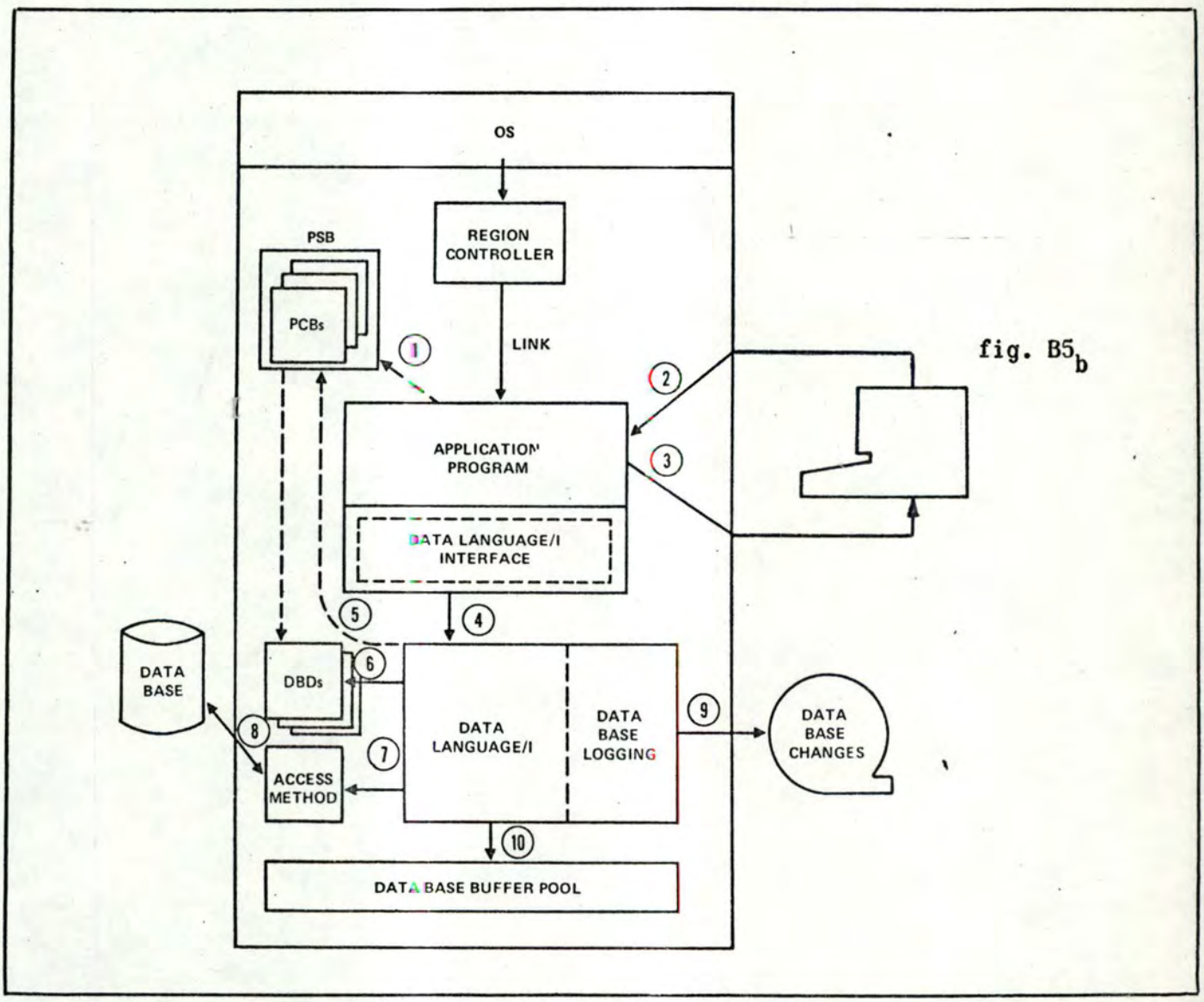
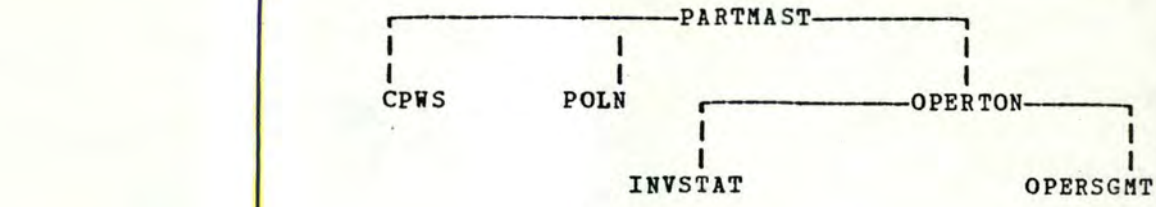


fig. $B5_b$




```
SAMPLE 1:

PCB     TYPE=TP,NAME=OUTPUT1
PCB     TYPE=TP,NAME=OUTPUT2
PCB     TYPE=DB,DBDNAME=PARTMSTR,PROCOPT=A,KEYLEN=100
SENSEG  NAME=PARTMAST,PARENT=0,PROCOPT=A
SENSEG  NAME=CPWS,PARENT=PARTMAST,PROCOPT=A
SENSEG  NAME=POLN,PARENT=PARTMAST,PROCOPT=A
SENSEG  NAME=OPERTON,PARENT=PARTMAST,PROCOPT=A
SENSEG  NAME=INVSTAT,PARENT=OPERTON,PROCOPT=A
SENSEG  NAME=OPERSGMT,PARENT=OPERTON
PSBGEN  LANG=COBOL,PSBNAME=APPLPGM1
END
```

fig. B_6

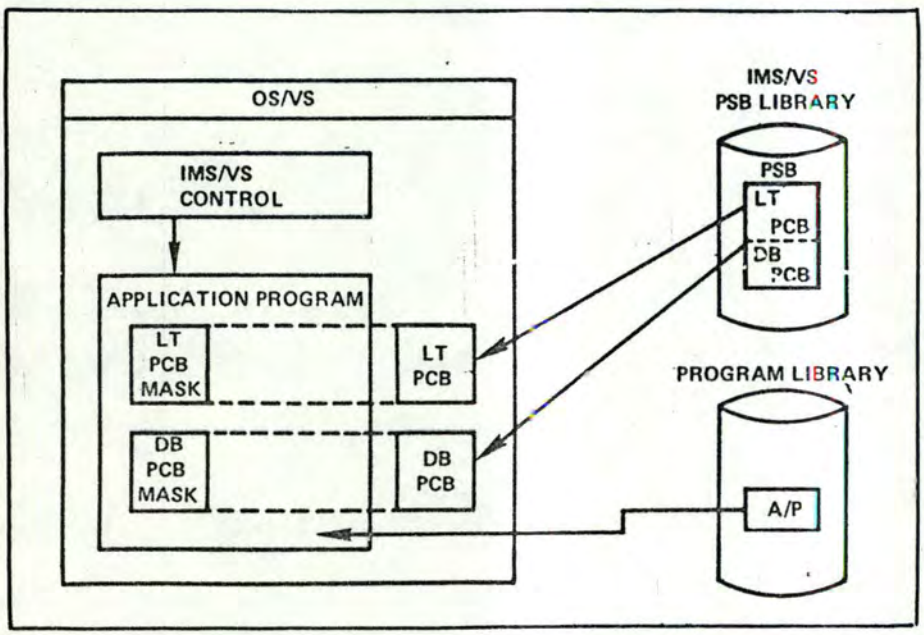
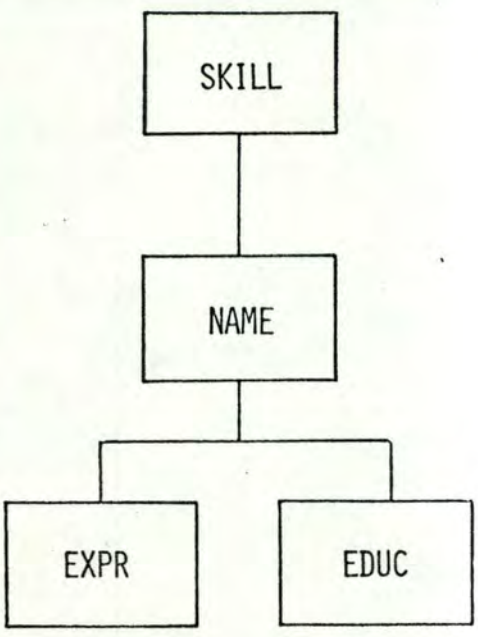


fig. B_7




```
DBD     NAME=SKILLINV,ACCESS=HISAM
DATASET DD1=SKLHISAM,OVFLW=HISAMOVF,DEVICE=2314

SEGM    NAME=SKILL,BYTES=31,FREQ=100
FIELD   NAME=(TYPE,SEQ,U),BYTES=21,START=1,TYPE=C
FIELD   NAME=STDCODE,BYTES=10,START=22,TYPE=C

SEGM    NAME=NAME,BYTES=20,FREQ=500,PARENT=SKILL
FIELD   NAME=(STDCLEVL,SEQ,U),BYTES=20,START=1,TYPE=C

SEGM    NAME=EXPR,BYTES=20,FREQ=10,PARENT=NAME
FIELD   NAME=PREVJOB,BYTES=10,START=1,TYPE=C
FIELD   NAME=CLASSIF,BYTES=10,START=11,TYPE=C

SEGM    NAME=EDUC,BYTES=75,FREQ=5,PARENT=NAME
FIELD   NAME=GRADLEVL,BYTES=10,START=1,TYPE=C
FIELD   NAME=SCHOOL,BYTES=65,START=11,TYPE=C

DBDGEN
FINISH
END
```

fig. B_8

BI.4.3. INTEGRITE

IMS/VS assure l'intégrité des données par divers moyens :

1. en isolant le programme de contrôle des programmes d'application, au niveau de l'architecture du système IMS

2. au moyen de la fonction "PROGRAM ISOLATION" : toute activité d'un programme d'application en cours d'exécution est isolée des programmes d'application actifs à ce moment, jusqu'à ce qu'il signale, en passant par un point de synchronisation, que les données qu'il a modifiées ou créées sont valides. Il est ainsi possible d'éviter des situations de blocage (DEADLOCK).

   exemple : cas de mise à jour d'un même segment concurremment par plusieurs programmes :

   . le terminal I est occupé à mettre à jour les segments A et B pendant qu'un terminal 2 essaye concurremment de modifier A à partir d'informations de B.

3. en permettant l'indépendance des données :

   . par rapport aux bases de données :
   les programmes accèdent aux données par leur nom (nom de segment) sans connaître :

   - comment et où sont mémorisées ces données ;
   - la méthode d'accès utilisée ;
   - éventuellement l'adresse physique employée.

   . par rapport aux terminaux :
   le programme adresse le terminal par nom (terminal logique) sans connaître le dispositif correspondant. Celui-ci est défini par le système et peut être changé dynamiquement.
   L'application est donc indépendante des caractéristiques physiques du terminal utilisé.

4. en fournissant des fonctions de :

   . CHECKPOINT/RESTART

   . RECOUVREMENT

   . Encodage/décodage des données (techniques cryptographiques) avant de les écrire/lire sur le support.

BI.4.4. DONNEES STATISTIQUES ET PROCEDURE DE VERIFICATIONS.

Destinées au responsable de la sécurité, ces données fournissent une trace de toutes les activités à l'intérieur du système :

- . utilisation des ressources par une application donnée ;
- . liste des activités pour chaque transaction ;
- . liste des tentatives d'accès non autorisés.

Remarque : en cas de tentative d'accès interdit, le responsable de la sécurité a le choix entre :

- . ne pas avertir le terminal principal;
- . avertir le terminal principal au moment de la tentative de violation ;
- . ne l'avertir qu'après un certain nombre de tentatives (défini préalablement pour chaque terminal) ne donnant lieu à aucune entrée valide afin d'éviter d'avertir le responsable pour une simple erreur de frappe.

BI.4.5. JOURNALISATION ET CONSTITUTION DE LISTES DE CONTROLE. (JOURNALLING/LOGGING)

BI.4.5.I. JOURNALISATION

Elle consiste à mémoriser sur une bande "journal" :

- . les transactions et commandes sans leur mot de passe en provenance des terminaux ;
- . toutes modifications apportées à la base de données.

A tout instant, le système peut donc être redémarré et la base de données restaurée dans son état initial.

Exemple :. Si la base de données a été détruite suite à une erreur d'entrée/sortie, la procédure de restauration sera la suivante :

1. Restauration de la base de données à l'aide d'une copie précédente, exécutée par les utilitaires de réorganisation de la base.
2. Application de toutes les modifications apportées à la base depuis la copie qui a servi à recharger la base. (système de recouvrement IMS/VS - voir BI.4.7.)
3. Exécution du programme qui a été interrompu, depuis le début de celui-ci, à partir des transactions et commandes de la bande "journal".

BI.4.5.2. LOGGING.

L'opération de logging sert à consigner (en temps réel) sur un fichier de sauvetage :

. des points de contrôle pris de temps à autre. (BI.4.6.)

. toutes les tentatives de violation de la sécurité c'est-à-dire, dans le cas :

- d'entrée d'un message à partir d'un terminal non autorisé,
- de mot de passe incorrectement introduit,
- d'absence de mot de passe, quand il est obligatoire,
- de commande interdite ou de code transaction inexistant etc...

IMS/VS rejette toute transaction incorrecte en envoyant un message au terminal qui l'a envoyée. En cas d'atteinte grave à la sécurité, le terminal sera bloqué jusqu'à la réception d'un ordre de redémarrage en provenance du terminal du responsable de la sécurité.

BI.4.6. POINT DE CONTROLE ET DE REPRISE.

BI.4.6.1. CONDITIONS PROVOQUANT UN CHECKPOINT.

Les conditions suivant lesquelles IMS provoquera la prise d'un checkpoint peuvent être groupées en quatre classes :

I. Checkpoints pris automatiquement par le système d'après le volume des messages.

2. Prise d'un checkpoint suivant une demande du terminal principal.du système sur un ordre d'arrêt.

3. Sur un ordre d'arrêt du système.

4. Le terminal principal demande de produire une copie de l'état actuel des données de la base.

BI.4.6.2. REPRISE (RESTART)

Le restart assure la reconstruction du système en cas :

- d'arrêt déterminé préalablement,
- d'arrêt imprévu,
- de destruction hardware (ex : destruction d'un disque ou erreur machine) ou software (ex.: perte de liens de chaînage) de la base de données.

autres exemples :-destruction de la file d'attente des messages,
-perte d'informations dans la mémoire principale.

Note : Un checkpoint est généralement constitué d'un ensemble de tables ou blocs représentant un état défini du système. Il est normalement conservé sur une bande de sauvetage.

BI.4.7. DEDOUBLEMENT DE LA BASE DE DONNEES ET RECOUVREMENT (BACKUP/RECOVERY

Le processus de dédoublement de la base de données associé à celui de recouvrement ainsi qu'à la prise de point de contrôle en vue d'un redémarrage du système, constituent les objectifs fondamentaux d'IMS.

Différentes procédures peuvent être prises en considération :

. Duplication de la bande "journal" et des autres bandes de sauvetage pour s'assurer qu'une panne d'un dispositif quelconque n'affectera pas la restauration de la base de données.

. Recouvrement des files d'attente :

. des messages n'ayant encore subi aucun traitement,

. des messages résultant d'un traitement et destinés à des terminaux.

En cas de panne hardware ou software, ceci évitera lors du restart ;

. de demander aux terminaux de réintroduire à nouveau les transactions perdues lors de la panne,

. de reconstituer les messages de sortie.

. Recouvrement de la base de données à partir : (voir Fig. B9.)

. de la bande journal,
. d'une copie intacte de la base.

. Rejet automatique, en cas d'interruption (abend) d'un programme, des modifications qu'il a voulu apporter à la base car :

. les données peuvent avoir été mises à jour incorrectement,
. le système ne peut en déterminer la validité. Il faut donc pouvoir redémarrer après correction du programme à un point garantissant la validité des données de la base.

Note : Point très important pour l'intégrité des données.

. Enregistrement du contenu de la mémoire principale, sur une bande de sauvetage en cas de panne de courant au moyen d'un dispositif hardware. Celui-ci permet, en outre, de continuer un certain temps avant l'arrêt définitif.

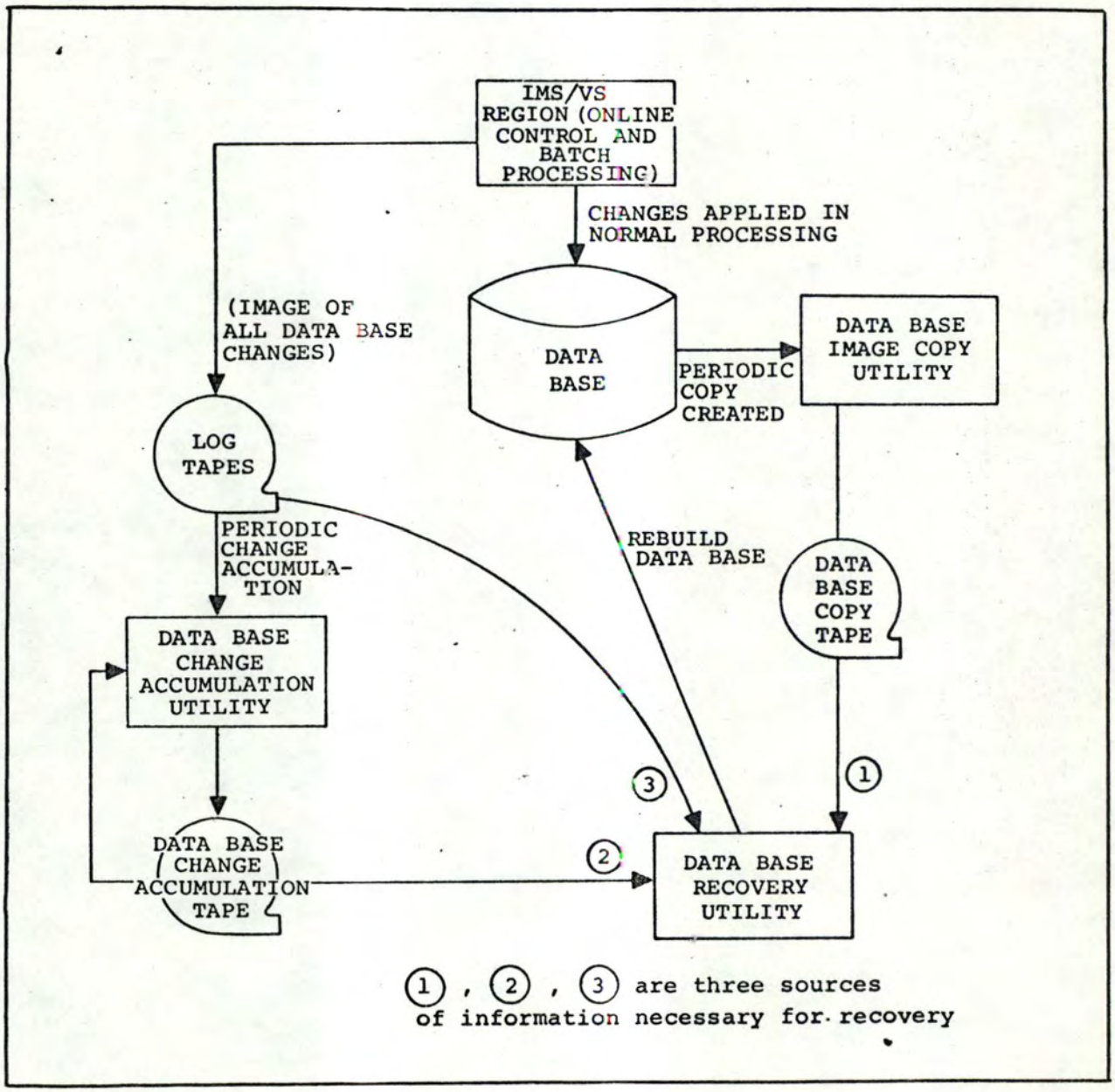

IMS/VS REGION (ONLINE CONTROL AND BATCH PROCESSING)
CHANGES APPLIED IN NORMAL PROCESSING
(IMAGE OF ALL DATA BASE CHANGES)
DATA BASE
PERIODIC COPY CREATED
DATA BASE IMAGE COPY UTILITY
LOG TAPES
PERIODIC CHANGE ACCUMULA-TION
REBUILD DATA BASE
DATA BASE COPY TAPE
DATA BASE CHANGE ACCUMULATION UTILITY
DATA BASE CHANGE ACCUMULATION TAPE
DATA BASE RECOVERY UTILITY
1
2
3
1 , 2 , 3 are three sources of information necessary for recovery

fig. B_9

BI.4.8. ADMINISTRATION

BI.4.6.I. NECESSITE D'UNE CENTRALISATION

Pour être efficace, elle ne doit pas être laissée au programmeur d'application ou à l'utilisateur du terminal.

BI.4.6.2. FONCTIONS PRINCIPALES : L'ADMINISTRATEUR DE LA BASE DE DONNEES/L'ADMINISTRATEUR DU SYSTEME DE COMMUNICATION DES DONNEES.

L'administrateur de la base de données définit :

- la structure de la base,
- la place physique des données,
- pour chaque programme : - le mode d'accès aux données,
  - les segments autorisés.
- différents utilitaires.

L'administrateur du système de communication de données :

- définit les liens entre terminaux logiques et physiques
- assigne les codes transactions aux programmes,
- assigne les mots de passe aux codes transactions et aux commandes.

BI.4.6.3. ROLE DU "MASTER TERMINAL".

Le terminal principal est un terminal privilégié qui contrôle et gère tous les autres terminaux du réseau relié au système IMS. Il a la possibilité d'entrer des commandes spéciales (/ASSIGN, /CHANGE, /DELETE, /DEQUEUE, /START, /STOP...) pour démarrer ou arrêter les terminaux, les programmes, ou pour prendre un point de contrôle et de reprise du système (/CHECKPOINT, /DBRECOVERY...).

Note : Puisque le terminal principal est un terminal logique, son statut peut être dynamiquement réassigné à un autre terminal physique. En cas de panne, par exemple, la console du système d'exploitation pourra être utilisée.

BI. 5 CONCLUSIONS.

C'est un des objectifs fondamentaux d'IMS de fournir différentes fonctions de protection permettant d'assurer la sécurité de la base de données (protection de l'accès et sauvegarde de l'intégrité des données). Il est évident qu'elles devront mettre en application les politiques de sécurité et de confidentialité des données définies par les responsables de l'entreprise.

La fonction d'administration (définie précédemment en BI.4.8.) sera accomplie :

- en interprétant judicieusement ces politiques lors de la conception du système et des applications,
- en fournissant des directives pour les phases suivantes :
  - définition du système,
  - génération des blocs de spécification du programme,
  - génération de la description de la base,

. programme de maintenance de la sécurité,
. programme d'analyses statistiques.

Bien qu'IMS fournit un ensemble de fonctions, certaines libertés sont laissées à l'utilisateur, notamment par le fait que :

- plusieurs fonctions sont facultatives :
  exemple : l'usage d'un "data base description block" (DBD) d'un PSB ou d'un code transaction est obligatoire. L'utilisation des mots de passe et d'un plan d'autorisation est facultative.
- des procédures supplémentaires peuvent être facilement insérées aux endroits nécessitant un contrôle plus étroit :
  exemple ; routine de test du n° d'identification de l'utilisateur.

B2. SECURITE DES DONNEES EN IDS.

B2. I INTRODUCTION

IDS est un langage qui permet à son utilisateur de définir une structure de fichier et d'implémenter un système de mémorisation et de recherche d'informations approprié à l'application spécifique de l'utilisateur. Il est conçu pour être utilisé conjointement avec un langage hôte (ex. : COBOL) et est opérationnel aussi bien en batch qu'en on-line.

B2. 2 FONCTIONS D'IDS ASSURANT LA SECURITE DES DONNEES.

B2.2.I. PROTECTION DES DONNEES.

A. AU NIVEAU DE LA DEFINITION DES DONNEES : CLAUSE AUTHORITY

La protection des données est réalisée au moyen de la clause AUTHORITY au niveau de la définition de l'enregistrement (niveau 01 en cobol). Cette clause facultative permet de fournir une valeur entière, inférieure à 4095, qui sera utilisée comme code de sécurité pour tous les enregistrements de ce type.
Ce code permet à un utilisateur de protéger ses données contre une lecture ou une mise à jour non autorisées.

Remarque :.Puisque ce code est identique pour tous les enregistrements d'un même type, il n'est pas inclu dans les données de ceux-ci, voir fig. BI0) mais dans la structure de définition (DEFINITION STRUCTURE) constituée par IDS pour chaque base de données (voir Fig. BII). Il existe de même une structure de définition pour chaque programme utilisateur : le transalateur IDS crée à l'intérieur de chaque programme source, une IDS-STRUCTURE-SECTION destinée à contenir la DEFINITION STRUCTURE (excepté le communication control block) associée à ce programme.

.L'organisation de la structure de définition est représentée à la Fig. BII :

- les rectangles représentent des entrées dont le format machine est un bloc de caractéristiques : (voir $BI2_a$ et b)
  - . description des enregistrements,
  - . relations entre enregistrements maîtres et détails,
  - . caractéristiques des chaînes,
  - . caractéristiques de contrôle.
- le code de sécurité associé éventuellement à chaque type d'enregistrement se retrouve :
  - . d'une part, dans le bloc de contrôle des communications qui sert d'intermédiaire, pour les données, entre le programme de l'utilisateur et les routines IDS. ($BI2_a$)

    (N.B.) au moment de l'exécution, la zone Authority remplie lors de la création de l'enregistrement sera comparée à la clé fournie par l'utilisateur dans l'ordre OPEN du DML. (DATA MANIPULATION LANG.)
  - . et d'autre part, dans chaque entrée définissant un type d'enregistrement (RECORD DEFINITION. Pour chaque type d'enregistrement, il existe un bloc de caractéristiques représenté à la Fig;BI2b.

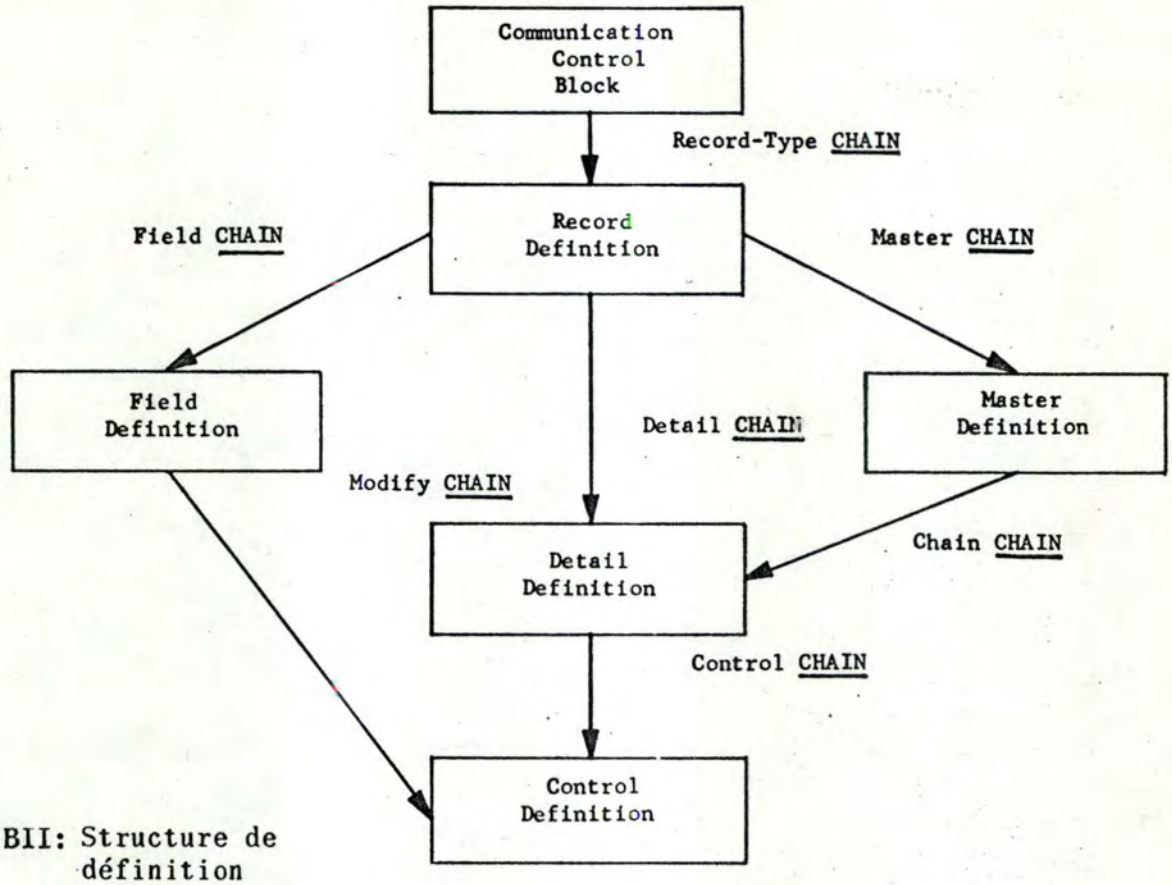


fig. BII: Structure de définition

Bits

	0	5	11	17	23	29	35
LOC-CCB	0 0	MBZ	DIRECT-REFERENCE				
+1	MBZ		FIRST-REFERENCE				
+2	MBZ		LAST-REFERENCE				
+3	MBZ		Record Type				
+4	Record Type Chain Next			MBZ	File Code		
+5	MBZ			ERROR-REFERENCE			
+6	MBZ	AUTHORITY		MBZ		OPEN Mode	

fig. $BI2_a$: Format du bloc de contrôle des communications

	0	5	8	11	17	29	35
LOC-SYM	0 1	MBZ	Record Type		Record Size	MBZ	S P R
+1	Page Interval				Master Chain Next		
+2	Field Chain Next				Detail Chain Next		
+3	Authority		Current Record Reference Code				
+4	Record Type Chain Next				MBZ		
+5	Minimum Page Range				Maximum Page Range		

fig. $BI2_b$ Format du bloc de de définition d'un enrégistrement

B. AU NIVEAU DU DATA MANIPULATION LANGUAGE.

A l'exécution, un utilisateur ne peut accéder à un enregistrement protégé qu'en ayant fourni préalablement la clé correspondant au type de celui-ci. Dans le cas contraire, la procédure de lecture ou d'écriture se terminera par le renvoi d'un code condition (ERROR CONDITION) au programme utilisateur.

Le code sécurité (ou la clé) est fourni par l'instruction OPEN (en PROCEDURE DIVISION du COBOL par exemple).

Note : IDS offre la possibilité de modifier la procédure de validation de l'accès pour l'adapter aux besoins de l'installation de l'utilisateur.

Format :

```
OPEN [ FOR { RETRIEVAL } ] [WITH AUTHORITY-KEY integer-1]
           { UPDATE    }
```

Remarque : Si le fichier IDS n'est ouvert qu'en mode RETRIEVAL, toute tentative d'utilisation d'une instruction STORE, DELETE, MODIFY ou UPDATE provoquera le renvoi d'une ERROR CONDITION au programme de l'utilisateur.

B2.2.2. INTEGRITE DES DONNEES

L'intégrité des données est réalisée par :

B2.2.2.I. POSSIBILITE D'ACCES CONCURRENTS A UN ENSEMBLE DE DONNEES COMMUNES.

Ceci peut être obtenu de deux façons différentes :

I. UTILISATION DE LA PROCEDURE "MULTI-ACCESS IDS PROTECTION"

Cette procédure nécessite de spécifier :

a) lors de la création d'un fichier : (base de données)
   . mode d'accès CONCURRENT
   . option MULTIUSER/YES/.

b) lors de la rédaction d'un programme utilisateur :
   . instruction INHIBIT (DML) :

   ° L'instruction INHIBIT est utilisée conjointement avec l'instruction ENABLE par les programmes qui veulent accéder à des fichiers permanents IDS nécessitant la protection multi-accès.

   ° Elle permet d'empêcher temporairement (jusqu'à l'instruction ENABLE) le partage de fichiers IDS. Tout programme suspendu par l'exécution de cette instruction devra attendre :
   - que tous les fichiers nécessaires à son exécution soient disponibles et réservés à son usage exclusif.

. instruction ENABLE (DML):

° Permet le partage de fichiers précédemment réservés par une instruction INHIBIT.

Voyons, par un exemple, comment utiliser ces instructions :

Trois utilisateurs veulent consulter la base de données, un autre veut la modifier. Ce dernier, avant de faire sa modification, lance un INHIBIT, ce qui exclut toute consultation ; la modification terminée, le lancement d'un ENABLE rendra la consultation possible pour les autres utilisateurs.

2. UTILISATION DU CONCEPT DE DEFINITION ET D'ALLOCATION DE SOUS-FICHIERS.

a) Définition : Un sous-fichier est un ensemble de pages à l'intérieur d'un fichier. En fait, ce sera, soit le fichier entier, soit une partie de celui-ci.

b) Remarques :. Les procédures du FILE SYSTEM ACTIVITY permettent la création, modification et suppression des sous- fichiers d'un fichier IDS.

. Au moment de l'exécution, l'utilisateur doit spécifier les sous-fichiers qui doivent être alloués à son programme. Il n'est pas possible d'interroger ou de mettre à jour concurremment un même sous-fichier, mais il est possible d'appliquer concurremment une fonction pour chaque sous- fichier.
exemple : s'il y a n sous-fichiers, il est possible de lancer soit n interrogations, soit n mises à jour concurremment ou encore de combiner celles-ci entre elles.

B2.2.3. JOURNALISATION :

Consiste en un archivage automatique de toutes les transactions de pages de la base de données.
Des informations en provenance des différents programmes en cours d'exécution sont stockées sur une bande journal (STATISTICAL COLLECTION FILE) ainsi qu'une copie des pages avant et après modification.

Ce seul fichier source sera utilisé pour rétablir la base de données dans l'état précédant l'événement qui a provoqué la perte d'intégrité.

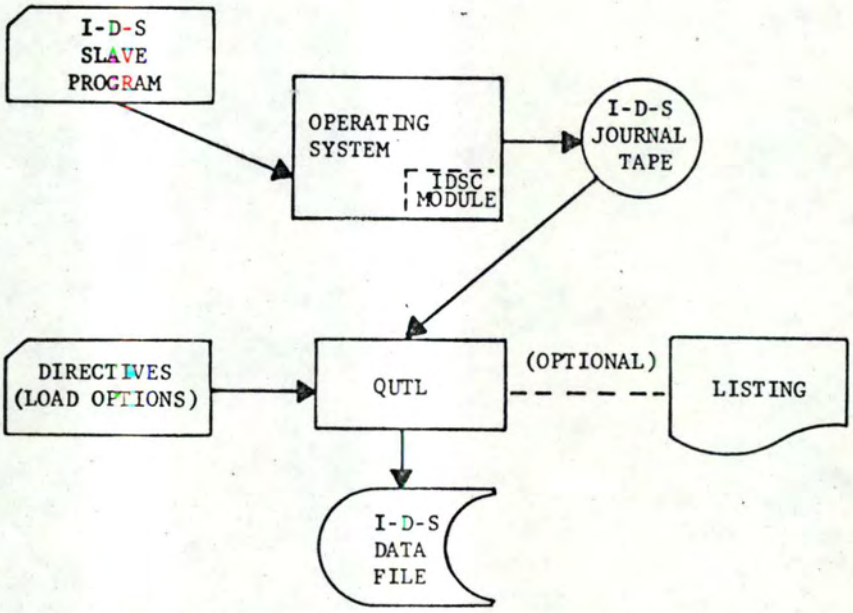
B2.2.4. PROCEDURE DE RECOUVREMENT ET/OU DE REPRISE (voir Fig. BI3)

Durant l'exécution d'un programme utilisateur, le système crée sur la bande journal :

° une copie de la page (BEFORE PAGE) avant qu'elle ne soit modifiée pour la première fois,
° une copie (AFTER PAGE) après modification dès que celle-ci a été réécrite dans la base.

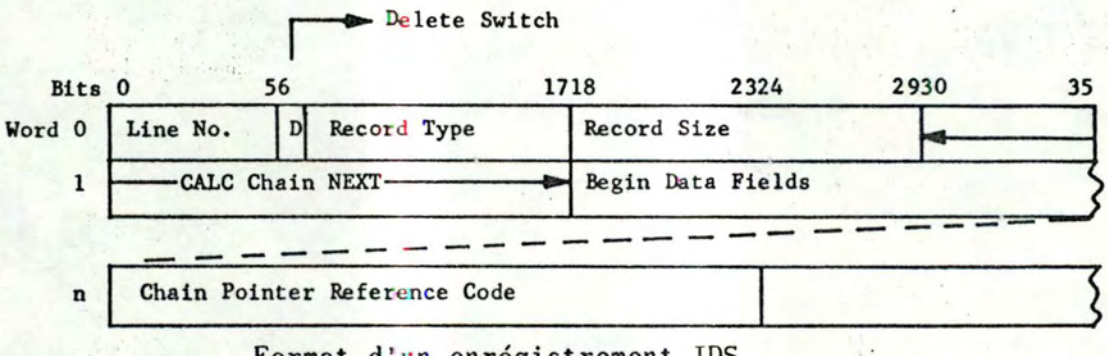
Chaque copie est accompagnée d'informations permettant d'identifier le programme en cours de traitement.

Si une opération de mise à jour se termine anormalement, le



Procédure de recouvrement

fig. B_{13}



Format d'un enrégistrement IDS

fichier IDS (ou le sous-fichier) est mis dans l'état de "fin anormale" (ABORT STATUS). Tant que la procédure de recouvrement n'est pas terminée, il restera inaccessible aux autres programmes.

Description de la procédure : deux options se présentent au responsable chargé de lancer la procédure de recouvrement :

- soit recopier les pages avant modification (BEFORE PAGE) dans l'ordre inverse de leur création, afin de reconstituer le fichier dans l'état où il était lors d'un point de contrôle (CHECKPOINT) précédent.

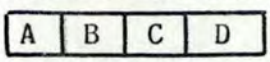
  exemple : cas d'un programme interrompu à cause d'une erreur provenant du programme.

- soit recopier les pages modifiées dans l'ordre de leur création afin de reconstituer le fichier dans l'état où il était juste avant l'erreur.

B2.3 CONCLUSIONS.

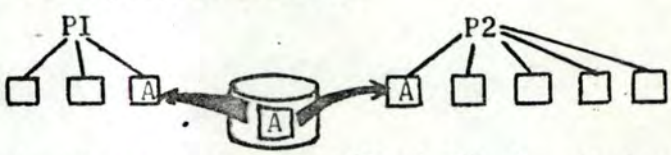
La protection Multi-accès n'est pas automatique en IDS. c'est l'utilisateur lui-même qui doit assurer cette protection en lançant les commandes INHIBIT et ENABLE; de ce fait, (si l'utilisateur ne lance pas ces commandes) il n'est pas toujours possible de déterminer à priori, le contenu d'un enregistrement modifié concurremment par des programmes différents.

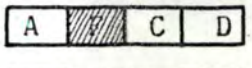
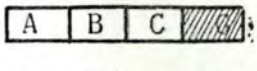
Exemple : si nous considérons les programmes PI et P2 ; chaque programme veut modifier R situé dans la page A.

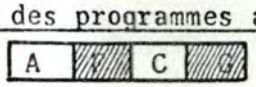


- PI modifie B en F dans l'enregistrement R ;
- P2 " D "G " " R ;

- Fonctionnement : Chaque programme reçoit la page A dans un de ses propres buffers.



- S'il y a eu concurrence entre PI et P2, le résultat final sera le suivant :
  - si aucun des programmes n'a lancé un "inhibit" :
    - soit  si PI se termine après P2
    - soit  si P2 se termine après PI
  - si l'un des programmes a lancé un "inhibit" :



On constate par cette étude, que la sécurité n'a pas été un des objectifs principaux dans la conception d'IDS. La principale raison réside dans le fait qu'IDS n'a pas été orienté, dès le départ, vers des applications de télétraitement.

UN PROJET DE LOI BELGE sur les fichiers de personnes

CHAPITRE 1" - LES ECOUTES ET PRISES DE VUE.

CHAPITRE II - LES BANQUES DE DONNEES ELECTRONIQUES

Art. 11.

Sont soumises aux dispositions du présent chapitre les banques de données électroniques.

Par banque de données électronique, on entend, au sens de la présente loi, tout système de traitement électronique de données, relevant du secteur public ou du secteur privé, relatives aux personnes physiques ou morales, et contenant le nom, la raison sociale ou la dénomination, le numéro personnel ou toute autre indication susceptible d'identifier la personne.

Les personnes morales, à savoir les associations et surtout les entreprises, entrent dans le champ de la loi, alors que la plupart des autres projets (et la loi suédoise) ne concernent que les personnes physiques.*

LA CREATION : LES AUTORISATIONS

Art. 12.

La création d'une banque de données électronique est subordonnée à l'autorisation de la Commission de contrôle de l'informatique instituée par l'article 26 de la présente loi.

Cette autorisation est accordée lorsqu'il n'existe aucun motif de craindre une atteinte abusive à la vie privée des personnes reprises dans la banque de données électronique.

La délivrance d'une autorisation pose le problème de l'instance habilitée à la délivrer, de la normalisation des banques de données et de toute l'infrastructure nécessaire au contrôle.

Art. 13.

Les décisions de la Commission de contrôle de l'informatique relatives aux autorisations sont susceptibles de recours auprès du Ministre de la Justice.

Le recours doit être formé dans les quinze jours de la notification de la décision.

Art. 14.

La Commission de contrôle de l'informatique tient à jour un registre des autorisations accordées.

Ce registre contient, pour chaque banque de données électronique :

1° le nom, la raison sociale ou la dénomination de la personne responsable de la banque de données électronique ;

2° le lieu d'implantation de la banque ;

3° le but et la nature des données traitées par la banque ;

4° les catégories de personnes admises à obtenir les données.

Toute personne peut consulter ce registre.

On retrouve là une notion fondamentale : le droit pour chacun de savoir ce que l'on sait sur lui.

Art. 15.

Tout changement dans l'utilisation de la banque de données électronique doit être notifié par la personne responsable de la banque, dans le délai d'un mois, à la Commission de contrôle de l'informatique, par une déclaration de modification, à consigner sur le registre prévu par l'article 14.

Ce changement est soumis à autorisation conformément à l'article 12 de la présente loi.

Art. 16.

§ 1. Sauf motifs exceptionnels, l'autorisation de faire figurer, dans une banque de données électronique, des données pouvant être à la source de discrimination pour la personne concernée, ne sera pas accordée.

Il en sera ainsi notamment des données relatives à la race, au sexe, aux opinions politiques, aux activités syndicales, aux convictions philosophiques ou religieuses.

§ 2. Les dispositions du paragraphe précédent n'interdisent pas à une association d'établir la liste de ses propres membres.

Art. 17.

L'autorisation de créer une banque de données électronique ne peut être accordée que pour des motifs exceptionnels lorsque, dans cette banque, figure l'une des données suivantes :

1°) les infractions dont une personne est soupçonnée ou pour lesquelles elle a été condamnée ;

2°) les mises à la disposition du gouvernement prévues par les articles 13 et 14 de la loi du 27 novembre 1891 pour la répression du vagabondage et de la mendicité ;

3°) les mesures prises à l'égard des mineurs par application des lois du 10 mai 1912 et du 8 avril 1965 ;

4°) les déchéances de la puissance paternelle prononcées par les tribunaux de la jeunesse ou les chambres de la jeunesse ;

5°) les internements à l'égard des anormaux et les mises à la disposition du gouvernement des récidivistes et des délinquants d'habitude ordonnés par application de la loi du 9 avril 1930 ou de la loi du 1er juillet 1964 ;

6°) les arrêtés de grâce (remises, réductions ou commutations de peines) ;

7°) les arrêtés ordonnant la libération conditionnelle ;

8°) les renvois de l'armée ;

9°) les déchéances de droits civils et politiques encourues par application des dispositions relatives à l'épuration civique ;

10°) les suspensions du prononcé des condamnations ordonnées par application de la loi du 29 juin 1964 concernant la suspension, le sursis et la probation ;

11°) les décisions judiciaires relatives à la faillite, au concordat ou au sursis de paiement ;

12°) les données relatives aux soins médicaux, à l'assistance sociale, aux traitements pour l'alcoolisme ou autres intoxications qu'une personne a reçus ;

13°) les données relatives à la filiation, à la séparation de corps ou au divorce.

Race, sexe, opinions politiques, religion, etc., constituent la « sphère des données sensibles » que tous les projets s'accordent à reconnaître inviolable. On y inclut parfois des informations d'ordre médical, militaire, judiciaire, etc.

Art. 18.

La Commission peut, par règlement soumis à l'approbation du Ministre de la Justice, déterminer la période au-delà de laquelle des données ne peuvent plus être gardées, utilisées ou diffusées.

Art. 20.

§ 1. L'autorisation accordée par la Commission de contrôle de l'informatique contient réglementation des points suivants :
1°) les buts poursuivis par la banque ;
2°) les données qui seront traitées électroniquement ;
3°) l'adaptation des données qui peut résulter de l'emploi d'un tel système de traitement ;
4°) les données qui pourront être portées à la connaissance des tiers.

§ 2. Cette autorisation peut en outre contenir réglementation des points suivants :
1°) les moyens utilisés pour la collecte des renseignements nécessaires à l'établissement de la banque de données électronique ;
2°) les méthodes d'application du traitement électronique de l'information ;
3°) les installations techniques ;
4°) les informations à fournir aux personnes reprises dans la banque ;
5°) la conservation des données ;
6°) le système de sécurité et de contrôle qui doit être mis en place avant la mise en exploitation de la banque de données électronique en vue de prévenir et de détecter les détournements de données, intentionnels ou non.

Ce point paraît soulever de grandes difficultés administratives ou techniques qui, souvent, font reculer le législateur. En fait, la loi suédoise montre qu'une normalisation de la déclaration (et donc des spécifications) rend possible la mise en application de telles dispositions.

Art. 21.

A la demande de la personne qui désire créer une banque de données électronique, la Commission de contrôle de l'informatique a l'obligation de délivrer une déclaration précisant si ladite banque doit donner lieu à autorisation ou à notification.

LE MAITRE DU FICHIER

Art. 22.

La personne responsable de la banque de données électronique doit faire toute diligence pour tenir les données à jour, pour corriger les données erronnées ou pour supprimer les données obtenues par des moyens illicites.

Art. 23.

La personne responsable de la banque de données électronique est tenue :
a) d'établir un état où sont consignés la nature des données enregistrées sur la personne, les buts dont la réalisation nécessite la connaissance de ces données ainsi que les destinataires habituels des données ;
b) de s'assurer du caractère approprié des systèmes de traitement des données ainsi que de la régularité de leur application ;
c) de faire connaître, par des mesures appropriées aux personnes participant aux traitements des données, les dispositions du présent chapitre, ainsi que les autres prescriptions relatives aux exigences particulières de la protection des données dans l'entreprise ou l'institution où ils travaillent.

Art. 24.

Les personnes responsables des banques de données électroniques ainsi que les personnes qui, dans l'exercice de leurs fonctions, ont connaissance des données enregistrées sont tenues au secret professionnel.

L'article 25 et les précédents introduisent la notion de personne responsable (« maître du fichier » dans la loi du Land de Hesse), disposition existant dans la loi suédoise. La personne responsable ne pourra, dans le cas d'une entreprise, être que le chef d'entreprise et non l'informaticien (salarié) « techniquement » responsable de la banque.

L'article 25 stipule que, à la demande, chacun pourra savoir ce que l'on sait sur lui et définit les modalités de l'accès à l'information.

LA COMMISSION DE CONTROLE

Art. 26.

Il est créé une Commission de contrôle de l'informatique chargée de veiller à ce que les systèmes de traitement électronique des données ne provoquent pas d'atteinte abusive à la vie privée.

La Commission de contrôle de l'informatique est un organisme autonome dont le siège est à Bruxelles.

Son règlement d'organisation est approuvé par le Roi.

Art. 27.

Les frais de fonctionnement de la Commission de contrôle de l'informatique sont à charge du budget du Ministère de la Justice.

Art. 25.

La Commission de contrôle de l'informatique est composée d'un Président et de douze membres nommés et révoqués par le Roi.

A partir de l'article 26 apparaît la notion de commission de contrôle (à laquelle pourtant il était fait allusion dès l'article 12). Remarquons qu'elle est nommée par le Roi : dans le cas du contrôle des banques de données publiques, se pose alors le problème de son indépendance par rapport au Pouvoir.

Le Président et les membres de la Commission ne peuvent être des responsables de banques de données électroniques.

Art. 29.

La Commission a, pour l'accomplissement de sa mission, tout pouvoir d'investigation auprès tant des services publics que des entreprises privées.

Les personnes responsables des banques de données électroniques sont tenues de lui fournir tous renseignements nécessaires à l'accomplissement de sa mission, notamment les informations relatives aux systèmes de traitement électronique auxquels elles recourent, les programmes de travail élaborés et l'exploitation des données obtenues.

La Commission peut requérir le concours d'experts et prescrire l'audition de tout responsable de banque de données électronique.

Art. 30.

Au cas où le fonctionnement d'une banque de données électronique constitue une atteinte abusive à la vie privée, la Commission de contrôle de l'informatique peut modifier où compléter les conditions auxquelles l'autorisation a été accordée.

Au cas où il s'avère impossible de faire cesser l'atteinte abusive à la vie privée par d'autres moyens, la commission peut annuler l'autorisation accordée en application de l'article 12 ou interdire la tenue d'une banque de données électronique notifiée conformément à l'article 19 § 3.

Art. 31.

§ 1. Sans préjudice de toutes voies de recours devant les tribunaux, la Commission examine les plaintes signées et datées qui lui sont adressées et par lesquelles lui est dénoncée toute utilisation des banques de données électroniques constituant une atteinte abusive à la vie privée.

§ 2. La Commission accuse réception de chaque plainte introduite et fait savoir à son auteur si elle estime que celle-ci est fondée ou non.

Art. 32.

Chaque année, à la date qu'elle détermine dans son règlement d'ordre intérieur, la Commission fait rapport au Ministre de la Justice.

Ce rapport est publié au Moniteur belge.

Sans être une instance judiciaire, la commission recevra les plaintes, sera tenue d'y apporter une réponse et, éventuellement, de saisir le pouvoir judiciaire. Il est surprenant, peut-être inquiétant, que relève de sa seule appréciation la recevabilité d'une plainte.

Les articles qui suivent (notamment 33) montrent qu'elle joue un rôle normatif au travers de ses recommandations et autres prescriptions.

Art. 33.

Indépendamment de son rapport annuel, la Commission notifie aux autorités administratives et aux entreprises privées les observations qu'elle croit devoir leur adresser. Elle s'enquiert auprès d'elles de la suite qui leur a été réservée.

(EXTRAIT de OI-HEBDO n° 313 du 16 décembre 1974)

Art. 34.

Sans préjudice de l'application de l'article 29 du Code d'instruction criminelle, ainsi que des obligations qui leur sont imposées par le présent chapitre et hors des cas où ils sont appelés à rendre témoignage en justice, les membres de la Commission de contrôle de l'informatique et les personnes relevant de son autorité ne peuvent se livrer à aucune divulgation des faits dont ils ont eu connaissance en raison de leurs fonctions.

Art. 35.

Le tribunal de première instance siégeant à Bruxelles est compétent pour connaître de toutes les contestations relatives au traitement électronique des données protégées par les dispositions du présent chapitre.

Art. 36.

Est puni d'un emprisonnement d'un an à cinq ans et d'une amende de mille francs à cent mille francs ou d'une de ces peines seulement :

1° quiconque a tenu une banque de données électronique sans l'autorisation prévue par le chapitre II de la présente loi lorsqu'une telle autorisation est nécessaire ou en contravention avec une interdiction prononcée conformément à l'article 30 ;

2° quiconque a tenu une banque de données électronique visée à l'article 19 sans l'avoir notifiée à la Commission de contrôle de l'informatique ;

3° quiconque a enfreint un règlement arrêté conformément aux articles 18, 20 ou 30 ;

4° quiconque a violé les dispositions des articles 24 ou 34 ;

5° quiconque ne fournit pas les renseignements ou donne des renseignements inexacts lors de la communication des renseignements visés à l'article 25 ;

6° la personne responsable d'une banque de données électronique qui ne donne pas accès aux locaux ou aux documents visés à l'article 29 ou qui ne remplit pas les obligations qui lui incombent aux termes des articles 22 et 23.

CHAPITRE IV : DISPOSITION TRANSITOIRE.

Art. 39.

Si une banque de données électronique qui, aux termes du chapitre II de la présente loi, ne peut être créée sans autorisation, est constituée avant la publication de la présente loi, sa tenue est autorisée jusqu'à ce que la demande d'autorisation ait été examinée définitivement, sous réserve que ladite demande ait été introduite avant le premier jour du douzième mois qui suit l'entrée en vigueur du chapitre II de la présente loi.

En ce qui concerne les banques de données électroniques visées à l'article 19, qui ont été constituées avant l'entrée en vigueur du chapitre II de la présente loi, la notification doit être adressée à la Commission de contrôle de l'informatique avant le premier jour du douzième mois qui suit l'entrée en vigueur du chapitre II de la présente loi.

L'article 39 qui vise la période dite transitoire se borne à entériner la situation actuelle où des fichiers de personnes existent (fichiers de personnel, de clients, fichiers des banques, des assurances) sans avoir été soumis à aucune autorisation.

LE PLAN GÉNÉRAL D'INFORMATIQUE DU SECTEUR PUBLIC ET LE REGISTRE NATIONAL DES HABITANTS DU ROYAUME

LA loi du 18 juillet portant approbation des « Lignes de force du Plan » contient un chapitre consacré au Plan général d'Informatique du secteur public. En voici les lignes maîtresses :

1. L'informatique du secteur public sera constituée en un système général et intégré.

2. Les informations primaires ne seront prélevées qu'une seule fois, le plus près possible de la source et élément par élément, avec un maximum de garanties de fiabilité, par le service le plus qualifié pour le faire. Ces informations primaires pourront cheminer dans le réseau et seront à la disposition des administrations et d'éventuels autres utilisateurs **à la seule condition que leurs échanges soient couverts par des dispositions légales et réglementaires.**

3. Le réseau comportera un nombre relativement réduit de centres de grande puissance, situés, soit à l'échelon central, soit à l'échelon régional et reliés entre eux par télécommunications.

4. On accèdera à ces centres par des périphériques.

LE REGISTRE NATIONAL

Le Registre national se place dans le cadre du programme prévu par la loi.

Sa mission essentielle consiste à **attribuer un numéro national** aux personnes physiques et morales, permettant ainsi qu'elles soient identifiées par un même indicatif dans tous les fichiers du pays.

Le Registre national poursuit cinq objectifs principaux :

1. permettre aux ordinateurs qui traitent des dossiers de personnes d'échanger entre eux des informations en fonction de programmes et sans intervention manuelle, une même personne étant identifiée de la même manière dans les divers ordinateurs ;

2. tenir à jour automatiquement l'identification et l'adresse des personnes de tous les fichiers qui y ont doit ;

3. mettre un ordinateur à la disposition des communes, même peu importantes, pour tous leurs problèmes de population ;

4. créer un inventaire permanent de la population, outil indispensable à la gestion d'un état moderne ;

5. supprimer de nombreuses prestations demandées aujourd'hui à la population, qui seront remplacées par des transferts d'information d'ordinateur à ordinateur.

Pour éviter les abus qui pourraient naître de l'extraordinaire pouvoir d'information que donne l'informatique organisée, nous avons voulu placer le Registre national dans un cadre légal.

Le projet de loi prévoit notamment :

a - la **limitation des informations qui seront enregistrées au Registre national**

Le Registre national ne pourra enregistrer que les informations reprises au registre de l'état-civil, au registre de la population et au registre des étrangers

b - la **limitation de l'accès au Registre national**

Auront accès au Registre national :

— les communes en ce qui concerne les informations qu'elles auront fournies ;

— les services publics, dans la mesure où la communication des informations qu'ils sollicitent est autorisée par les lois et règlements ;

— les personnes qui y sont inscrites pour les renseignement qui les concernent ;

— les tiers, selon la déclaration d'usage qu'ils auront à faire et dans les mêmes limites que celles auxquelles sont astreintes les autorités ou services publics dont les renseignements émanent ;

c - des **sanctions pénales** pour ceux qui contreviendraient à la loi.

Sur base du volontariat de plus de 80 % des communes, 7,5 millions de personnes sont déjà reprises au Registre national.

Le Registre national sera opérationnel peu de temps après le vote, par le Parlement, de la loi qui doit le consacrer.

Jules VANDENDRIES
Directeur Général du Service d'Administration Générale
Fonction Publique, Services du Premier Ministre.

D. LA DEONTOLOGIE DES INFORMATICIENS DES ADMINISTRATIONS PUBLIQUES

L'utilisation de l'ordinateur peut être limitée par des procédés techniques qui contrôlent notamment l'accès aux informations.

Cependant la maîtrise des machines ne suffit pas, et il faut prévoir des principes déontologiques qui s'imposeront aux informaticiens.

Cette déontologie s'organise autour de trois axes dans le cas des fonctionnaires (1)

1°- le respect de la loi, qui prescrit la confidentialité des informations détenues en fonction de l'activité professionnelle;

2°- le respect de l'information exige qu'on cherche à éviter des pertes ou des altérations au cours du processus informatique. Cette règle s'applique à tous les hommes qui collaborent au traitement des données, ce qui implique la réalisation d'un inventaire des tâches informatiques de l'administration et la description des devoirs qui s'imposent à chaque tâche, avant et après l'installation de l'ordinateur.

Ce sont les abus liés au traitement des données qui sont les plus spécifiques à l'informatique.

Ils peuvent se présenter avant même l'installation de l'ordinateur lorsque se font les études de hardware et de software qui détermineront le choix d'un matériel en fonction des besoins des administrations

Mais on songe surtout aux critères qui guident :

- le choix qu'on retiendra parmi les informations collectées,
- le recours aux "abstrats" qui restituent les informations sous une forme plus concise,
- le choix du langage spécifique adapté aux besoins qui permettra de "traiter" les données pour obtenir une réponse aux questions posées,
- la mise à jour des fichiers.

(1) Voir à ce sujet F. DELPEREE- "Les Hommes" dans "L'Informatique et l'administration"-Rapport belge au XVe Congrès International des Sciences Administratives. Rome, 6-11 septembre 1971

Au moment de la diffusion de l'information des erreurs peuvent résulter d'un manque de contrôle préalable de la pertinence des réponses de l'ordinateur aux questions posées.

Enfin, la transmission des résultats dépend des agents des services des télécommunications.

3°- le respect de la fonction publique s'impose aux informaticiens comme aux autres agents des services publics.
-La nécessité d'assurer la continuité du service, qui pose le problème du droit de grève, mérite une étude plus approfondie, compte tenu des revendications des agents des services publics en matière de droits syndicaux.

Répression de la transgression des règles de déontologie

La réparation civile et la répression pénale ont été envisagées à l'occasion de certaines études.

La caractère spécifique de la matière informatique justifie peut-être le recours à d'autres formules, comme l'ombudsman ou le comité paritaire de "sages", fonctionnaires et informaticiens.

(Extrait de "Les agents de l'état face à l'informatique" p 56-57 SCOKAERT, Alfred et autres)

BIBLIOGRAPHIE

A. LIVRES

J. MARTIN
"DESIGN of REAL-TIME Computer Systems"
PRENTICE-HALL, INC., ENGLEWOODS CLIFFS, N.J.

J. MARTIN
"SYSTEMS ANALYSIS FOR DATA TRANSMISSION"
"SECURITY, ACCURACY and PRIVACY in Computer Systems"
"Introduction to Teleprocessing"
PRENTICE-HALL, INC., ENGLEWOODS CLIFFS, N.J.

MARTIN and NORMAN
"The Computerized Society" PRENTICE-HALL

VAN TASSEL
"Computer Security Management" PRENTICE-HALL

STRANACK
"Real-Time International Computer state of the art report" (Bibl. Inform.)

YOURDON
"Design of ON-LINE COMPUTERS SYSTEMS" (Bibl. Inform.)

CENTI (F2)
"Gestion en temps Réel" (Bibli Inform.)

G. MESSADIE
"La fin de la vie privée" Ed. CALMANN-LEVY, 1974

CODASYL
"DATA BASE TASK GROUP" - Avril 71
"SYSTEMS COMMITTEE: FEATURE ANALYSIS OF GENERALIZED DATA BASE MANAGEMENT SYSTEMS" Technical report-Mai 71

J.P. WINDAL
"Cours de télétraitement de 2° licence et maîtrise" (Institut d'Inform.)

DE HEPCEE
"Cours temps-réel de 2° et 3° licence et maîtrise" (Institut d'inform.)

B. PUBLICATIONS ET REVUES, ARTICLES

DATAMATION (janvier 74)

"Computer security, an averview" Harold Weiss pp42-47
"Privacy, People and Credit Services" Robert L. Patrick pp48-50
"Software Security" Jacob Palme pp5I-55

DATAMATION (septembre 74)

"Directions in Data Base Management Technology" Richard F. Schubert pp49-5I
"The data base in a critical on-line business environment" pp52-56 G.E. HUTTN

DATAMATION (mai 70)

"Getting a personal dossier from a statistical data bank" L.J. HOFFMAN pp74-75

AFIPS-CONFERENCE PROCEEDINGS

"Security controls in the ADEPT-50 time-sharing systems" C. WEISSMAN
I969 FJCC Vol 35 pp II9-I33
"Protection-principles and practice" G.S. GRAHAM P.J. DENNING
I972 SJCC Vol 40 pp 4I7-429
"Privacy and Security in Databank Systems-Measures of Effectiveness, Costs, and Protector-Intruor Interactions" TURN FJCC,Vol 4I pp 435-444 I9732

"Insuring Confidentiality of Individual Record in Data Retrieval and Storage and Retrieval for Statistical Purposes" HANSEN M.H. FJCC Vol 39 I97I
"The Application of Cryptographic techniques to data processing"
R.O. SKATRUD FJCC Vol 35 pp III-II7 I969
"Multi-dimensional Security Program for a generalized information retrieval system" JOHN M. CARROL FJCC Vol 39 pp 57I-577 I97I
"The formulary model for flexible privacy and access controls"
J. LANCE FJCC Vol 39 pp 587-60I I97I

EDP-ANALYSER (janvier 74/ Vol I2 n° I)

"PROTECTING VALUABLE DATA(PART2)"

HONEYWELL COMPUTER JOURNAL

"Penetration of computer systems-an overview" D.J. BARTEK Vol 8 n°2 I974
"Encryption for data security" D.J. BARTEK "
"File encryption as a security tool" R.R. KEYS "

"The interactions of computer and Privacy" A.M. NOLL ppI63-I72 Vol 7 n°3 73

"LEGAL ASPECTS OF COMPUTERIZED INFORMATION SYSTEMS"
(Report to the Committee on Scientific and Technical Information of the Federal Council of Science and Technology US Government from its Panel on Legal Aspects of Information Systems) Vol 7 n°I I973

COMMUNICATION OF THE ACM

"Protection and the Control of Information Sharing in MULTICS" Juillet 74 pp 388-402
"A user Authentication Scheme Not Requiring Secrecy in the computer" Arthur Evans pp 437-44I Août 74/Vol I7/n°8
"Execution Time Requirements for Encipherment Programs"
T. D. FRIEDMAN pp 445-452 Août 74/Vol I7/n°8

OI-INFORMATIQUE (mensuel)

"Les systemes de gestion de bases de données" (parties I et 2)
n° 75 et 76 -janvier/février/mars 74- Claude SAULNIER
n° 84 -décembre 74
"Télétraitement: codification,transmission, gestion et traitement des messages"
n° 73 -novembre 73 pp25-29 B. BRULLER

INFORMATIQUE ET GESTION (mensuel)
"Banques de données: des responsabilités nouvelles" P. DUMAS n°52 novembre 73

BUREAU ET INFORMATIQUE (mensuel)
"La sécurité en informatique:Environnement de l'ordinateur" n°28 fév./mars 74

IBM- "IMS/VS GENERAL INFORMATION MANUEL" Mars 74 GH20-I260-I
"IMS/VS SYSTEM/APPLICATION DESIGN GUIDE" Févr. 74 SH20-9025-0

SLIGOS INTERFACE n°I0/I974
Editorial de Gérard Bauvin.

Firmes contactées: ----------

FICHET-BAUCHE /Département Contrôle d'accès/ (Mr. René E. WEGELIN)
(France)
FLAMBO (France) ; YAC CHAUVIN et BAUER (Sécurité informatique)
(SICOB/SEPTEMBRE 74) /sécurité physique/

EIPROS (France)/Terminaux et dispositifs de contrôle d'accès/ (J. PUENTE-CASTA

TRINDEL (FRANCE)/ Identimat 2000/ (Mr J. BERLOT)